

**INTELLIGENCE ACTIVITIES  
SENATE RESOLUTION 21**

---

---

**HEARINGS  
BEFORE THE  
SELECT COMMITTEE TO STUDY  
GOVERNMENTAL OPERATIONS WITH  
RESPECT TO INTELLIGENCE ACTIVITIES  
OF THE  
UNITED STATES SENATE  
NINETY-FOURTH CONGRESS  
FIRST SESSION**

---

**VOLUME 5**

---

**THE NATIONAL SECURITY AGENCY AND FOURTH  
AMENDMENT RIGHTS**

OCTOBER 29 AND NOVEMBER 6, 1975



Printed for the use of the Select Committee To Study Governmental  
Operations With Respect to Intelligence Activities

U.S. GOVERNMENT PRINTING OFFICE

67-522

WASHINGTON : 1976

---

For sale by the Superintendent of Documents, U.S. Government Printing Office  
Washington, D.C. 20402 - Price \$2.30

**SENATE SELECT COMMITTEE TO STUDY GOVERNMENTAL OPERATIONS  
WITH RESPECT TO INTELLIGENCE ACTIVITIES**

FRANK CHURCH, Idaho, *Chairman*  
JOHN G. TOWER, Texas, *Vice Chairman*

PHILIP A. HART, Michigan	HOWARD H. BAKER, JR., Tennessee
WALTER F. MONDALE, Minnesota	BARRY GOLDWATER, Arizona
WALTER D. HUDDLESTON, Kentucky	CHARLES MCC. MATHIAS, Jr., Maryland
ROBERT MORGAN, North Carolina	RICHARD SCHWEIKER, Pennsylvania
GARY HART, Colorado	

WILLIAM G. MILLER, *Staff Director*  
FREDERICK A. O. SCHWARZ, JR., *Chief Counsel*  
CURTIS R. SMOOTHERS, *Counsel to the Minority*  
AUDREY HATRY, *Clerk of the Committee*

## C O N T E N T S

---

### HEARING DAYS

	<b>Page</b>
Wednesday, October 29, 1975-----	1
Thursday, November 6, 1975-----	57

### LIST OF WITNESSES

#### WEDNESDAY, OCTOBER 29, 1975

Lieutenant General Lew Allen, Jr., Director, National Security Agency; accompanied by Benson Buffham, Deputy Director, NSA; and Roy Banner, General Counsel, NSA-----	5
---	---

#### THURSDAY, NOVEMBER 6, 1975

Edward H. Levi, Attorney General of the United States-----	84
Philip B. Heymann, Professor of Law, Harvard Law School-----	136

### HEARINGS EXHIBITS<sup>1</sup>

No. 1—October 20, 1967 cable from Lieutenant General William Yar- borough, ACSI, to Lieutenant General Marshall Carter, Director, NSA-----	145
No. 2—October 21, 1967 cable from Lieutenant General Marshall Carter, Director, NSA to USIB members-----	147
No. 3—July 1, 1969 memo from an Assistant Director, NSA, establishing Project MINARET as a Sensitive SIGINT Operation, and at- tached MINARET Charter-----	149
No. 4—April 10, 1970 memo from John E. Ingersoll, Director, Bureau of Narcotics and Dangerous Drugs, to Director, NSA-----	151
No. 5—January 26, 1971 memo from Vice Admiral Noel Gayler, Director, NSA, to the Secretary of Defense and the Attorney General-----	156
No. 6—September 17, 1973 letter from Lieutenant General Lew Allen, Jr., Director, NSA, to Clarence M. Kelley, Director, FBI-----	158
No. 7—October 1, 1973 letter from Attorney General Elliot Richardson to Lieutenant General Lew Allen, Jr., Director NSA-----	160
No. 8—October 4, 1973 letter from Lieutenant General Lew Allen, Jr., Director, NSA, to Attorney General Elliot Richardson-----	162

### APPENDIX

November 10, 1975 letter from Attorney General Levi to Senator Schweiker concerning discussion of FBI Manual of Instructions-----	164
--	-----

---

<sup>1</sup> Under criteria determined by the Committee in consultation with the White House, the Departments of Defense and Justice, the National Security Agency, and the Federal Bureau of Investigation, certain materials have been deleted from these exhibits, which were previously classified, to maintain the integrity of the internal operating procedures of the agencies involved, and to protect sensitive communications intelligence sources and methods. Further deletions were made with respect to protecting the privacy of certain individuals and groups.

# INTELLIGENCE ACTIVITIES—THE NATIONAL SECURITY AGENCY AND FOURTH AMENDMENT RIGHTS

---

WEDNESDAY, OCTOBER 29, 1975

U.S. SENATE,  
SELECT COMMITTEE TO STUDY GOVERNMENTAL OPERATIONS  
WITH RESPECT TO INTELLIGENCE ACTIVITIES,  
*Washington, D.C.*

The committee met, pursuant to notice, at 10:15 a.m., in room 318, Russell Senate Office Building, Senator Frank Church (chairman) presiding.

Present: Senators Church, Tower, Mondale, Huddleston, Morgan, Hart of Colorado, Baker, Goldwater, Mathias and Schweiker.

Also present: William G. Miller, staff director; Frederick A. O. Schwarz, Jr., chief counsel; Curtis R. Smothers, counsel to the minority.

The CHAIRMAN. The hearing will please come to order.

This morning, the committee begins public hearings on the National Security Agency or, as it is more commonly known, the NSA. Actually, the Agency name is unknown to most Americans, either by its acronym or its full name. In contrast to the CIA, one has to search far and wide to find someone who has ever heard of the NSA. This is peculiar, because the National Security Agency is an immense installation. In its task of collecting intelligence by intercepting foreign communications, the NSA employs thousands of people and operates with an enormous budget. Its expansive computer facilities comprise some of the most complex and sophisticated electronic machinery in the world.

Just as the NSA is one of the largest and least known of the intelligence agencies, it is also the most reticent. While it sweeps in messages from around the world, it gives out precious little information about itself. Even the legal basis for the activities of NSA is different from other intelligence agencies. No statute establishes the NSA or defines the permissible scope of its responsibilities. Rather, Executive directives make up the sole "charter" for the Agency. Furthermore, these directives fail to define precisely what constitutes the "technical and intelligence information" which the NSA is authorized to collect. Since its establishment in 1952 as a part of the Defense Department, representatives of the NSA have never appeared before the Senate in a public hearing. Today we will bring the Agency from behind closed doors.

The committee has elected to hold public hearings on the NSA only after the most careful consideration. For 23 years this Agency has provided the President and the other intelligence services with communications intelligence vital to decisionmaking within our Govern-

ment councils. The value of its work to our national security has been and will continue to be inestimable. We are determined not to impair the excellent contributions made by the NSA to the defense of our country. To make sure this committee does not interfere with ongoing intelligence activities, we have had to be exceedingly careful, for the techniques of the NSA are of the most sensitive and fragile character. We have prepared ourselves exhaustively; we have circumscribed the area of inquiry to include only those which represent abuses of power; and we have planned the format for today's hearing with great care, so as not to venture beyond our stated objectives.

The delicate character of communications intelligence has convinced Congress in the past not to hold public hearings on NSA. While this committee shares the concern of earlier investigative committees, we occupy a different position than our predecessors. We are tasked, by Senate Resolution 21, to investigate "illegal, improper, or unethical activities" engaged in by intelligence agencies, and to decide on the "need for specific legislative authority to govern operations of \* \* \* the National Security Agency." Never before has a committee of Congress been better prepared, instructed, and authorized to make an informed and judicious decision as to what in the affairs of NSA should remain classified and what may be examined in a public forum.

Our staff has conducted an intensive 5-month investigation of NSA, and has been provided access to required Agency files and personnel. NSA has been cooperative with the committee, and a relationship of mutual trust has been developed. Committee members have received several briefings in executive session on the activities of the Agency, including a week of testimony from the most knowledgeable individuals, in an effort to determine what might be made public without damaging its effectiveness. Among others, we have met with the Directors of the NSA and the CIA, as well as the Secretary of Defense. Finally, once the decision was made to hold public hearings on the NSA, the committee worked diligently with the Agency to draw legitimate boundaries for the public discussion that would preserve the technical secrets of NSA, and also allow a thorough airing of Agency practices affecting American citizens.

In short, the committee has proceeded cautiously. We are keenly aware of the sensitivity of the NSA, and wish to maintain its important role in our defense system. Still, we recognize our responsibility to the American people to conduct a thorough and objective investigation of each of the intelligence services. We would be derelict in our duties if we were to exempt NSA from public accountability. The committee must act with the highest sense of responsibility during its inquiry into the intelligence services. But it cannot sweep improper activities under the rug—at least not if we are to remain true to our oath to uphold the Constitution and the laws of the land.

We have a particular obligation to examine the NSA, in light of its tremendous potential for abuse. It has the capacity to monitor the private communications of American citizens without the use of a "bug" or "tap." The interception of international communications signals sent through the air is the job of NSA; and, thanks to modern technological developments, it does its job very well. The danger lies in the ability of the NSA to turn its awesome technology against domestic communications. Indeed, as our hearings into the Huston plan demon-

strated, a previous administration and a former NSA Director favored using this potential against certain U.S. citizens for domestic intelligence purposes. While the Huston plan was never fully put into effect, our investigation has revealed that the NSA had in fact been intentionally monitoring the overseas communications of certain U.S. citizens long before the Huston plan was proposed—and continued to do so after it was revoked. This incident illustrates how the NSA could be turned inward and used against our own people.

It has been the difficult task of the committee to find a way through the tangled webs of classification and the claims of national security—however valid they may be—to inform the American public of deficiencies in their intelligence services. It is not, of course, a task without risks, but it is the course we have set for ourselves. The discussions which will be held this morning are efforts to identify publicly certain activities undertaken by the NSA which are of questionable propriety and dubious legality.

General Allen, Director of the NSA, will provide for us today the background on these activities, and he will be questioned on their origins and objectives by the committee members. Like the CIA and the IRS, the NSA, too, had a "watch list" containing the names of U.S. citizens. This list will be of particular interest to us this morning, though we will take up another important subject as well. The dominant concern of this committee is the intrusion by the Federal Government into the inalienable rights guaranteed Americans by the Constitution. In previous hearings, we have seen how these rights have been violated by the intelligence services of the CIA, the FBI, and the IRS. As the present hearings will reveal, the NSA has not escaped the temptation to have its operations expanded into provinces protected by the law.

While the committee has found the work of the NSA on the whole to be of a high caliber and properly restrained and has tremendous respect for the professional caliber of the people who work there, the topics we shall explore today do illustrate excesses and suggest areas where legislative action is desirable. That is why we are here.

Senator Tower would like to make an opening statement.

Senator TOWER. Thank you, Mr. Chairman.

Mr. Chairman, I shall be brief. From the very beginning, I have opposed the concept of public hearings on the activities of the NSA. That opposition continues, and I should like to briefly focus on the reasons I believe these open hearings represent a serious departure from our heretofore responsible and restrained course in the process of our investigation.

To begin with, this complex and sophisticated electronic capability is the most fragile weapon in our arsenal; and unfortunately, I cannot elaborate on that, because that would not be proper. Public inquiry on NSA, I believe, serves no legitimate legislative purpose, while exposing this vital element of our intelligence capability to unnecessary risk, a risk acknowledged in the chairman's own opening statement.

S. Res. 21 does authorize the NSA inquiry, and this has been done very thoroughly in closed session. But that same resolution also picks up a recurring theme of the floor debate upon the establishment of this committee. Specifically, we were admonished not to disclose out-

side the committee information which would adversely affect intelligence activities. In my view, the public pursuit of this matter does adversely affect our intelligence-gathering capability.

Even if the risks were minimal—and I do not believe they are minimal—the NSA is the wrong target. The real quarry is not largely mechanical response of military organizations to orders. The real issues of who told them to take actions now alleged to be questionable should be addressed to the policy level. It is more important to know why names were placed on a watch list than to know what the NSA did after being ordered to do so.

In summary, Mr. Chairman, I believe we have fallen prey to our own fascination with the technological advances of the computer age. We have invited a three-star military officer to come before us to explain the awesome technology and the potential abuses of a huge vacuum cleaner. We have done this despite the fact that our exhaustive investigation has established only two major abuses in 23 years, both of which have been terminated. And despite the obvious risks of this sensitive component of the Nation's intelligence-gathering capability, I am opposed to a procedure which creates an unnecessary risk of irreparable injury to the public's right to be secure; even if offered under the umbrella of the acknowledged presumption of a citizen's right to know.

In taking such risks, we both fail to advance the general legislative purpose and, I believe, transgress the clearly expressed concerns of the Senate requiring us to, if we err at all, err on the side of caution. It is my view that there comes a point when the people's right to know must of necessity be subordinated to the people's right to be secure, to the extent that a sophisticated and effective intelligence-gathering capability makes them secure.

I do not think that any of us here, for example, would want us to sacrifice our capability for verification of Soviet strategic weapons capability. And whether or not that capability was thought posture in a first-strike configuration, I cite it only as an example. Hence, my opposition to the conduct of these public hearings.

I am aware, Mr. Chairman, that through the democratic process, the committee has, by a majority vote, voted to go this route. But I felt a compulsion to state my own reasons for being in opposition.

The CHAIRMAN. Senator Tower, I appreciate your statement, and I might say that there are two levels of concern in the committee, and relating to the two different practices that are of questionable legality. And so, we have divided this hearing into two parts, proceeding with the portion that has least objection from members of the committee who feel as Senator Tower does. And then, we will have an opportunity to discuss further the second part, after General Allen has left the witness stand. And that is the procedure, that is satisfactory with you?

Senator TOWER. I accept the procedure, and it is totally satisfactory to me.

The CHAIRMAN. Very well.

Now, General Allen has come prepared with his statement, after which, General, there will be questions from the committee. I wish you would identify those who will be sitting with you; and if they

might respond to questions, then I would ask them to stand with you to take the oath. Would you first identify them, please?

General ALLEN. Yes. On my right is Mr. Benson Buffham, who is the Deputy Director of the National Security Agency. On my left is Mr. Roy Banner, who is the General Counsel of the National Security Agency.

Sir, I suppose—or at least for our initial purposes—that I be the only witness.

The CHAIRMAN. Very well. Then you alone may stand and take the oath. Do you solemnly swear that all of the testimony you will give in this proceeding will be the truth, the whole truth, and nothing but the truth, so help you God?

General ALLEN. I do.

The CHAIRMAN. Thank you.

General, I know you have a prepared statement. Will you please proceed with it at this time.

**TESTIMONY OF LT. GEN. LEW ALLEN, JR., DIRECTOR, NATIONAL SECURITY AGENCY, ACCOMPANIED BY BENSON BUFFHAM, DEPUTY DIRECTOR, NSA; AND ROY BANNER, GENERAL COUNSEL, NSA**

General ALLEN. Mr. Chairman, members of the committee, I recognize the important responsibility this committee has to investigate the intelligence operations of the U.S. Government and to determine the need for improvement by legislative or other means. For several months, involving many thousands of man-hours, the National Security Agency has, I believe, cooperated with this committee to provide a thorough information base, including data whose continued secrecy is most important to our Nation.

We are now here to discuss in open session certain aspects of an important and hitherto secret operation of the U.S. Government. I recognize that the committee is deeply concerned that we protect sensitive and fragile sources of information. I appreciate the care which this committee and staff have exercised to protect the sensitive data we have provided.

I also understand that the committee intends to restrict this open discussion to certain specific activities and to avoid current foreign intelligence operations. It may not be possible to discuss all these activities completely without some risk of damage to continuing foreign intelligence capabilities. Therefore, I may request some aspects of our discussion be conducted in executive session where there can be opportunity to continue our full and frank disclosure to the committee of all the information you require. The committee may then develop an appropriate public statement. We are therefore here, sir, at your request, prepared to cooperate in bringing these matters before your committee.

In the interest of clarity and perspective, I shall first review the purpose of the National Security Agency and the authorities under which it operates. Next, I will describe the process by which requirements for information are levied on NSA by other Government agencies. And finally, I will give a more specific description of an operation conducted in 1967-73 by NSA in response to external requirements, which I will refer to as "the watch list activity." This ac-

tivity has been subject to an intensive review by this committee and staff in closed session.

Under the authority of the President, the Secretary of Defense has been delegated responsibility for both providing security of U.S. governmental communications and seeking intelligence from foreign electrical communications. Both functions are executed for the Secretary of Defense by the Director, National Security Agency, through a complex national system which includes the NSA as its nucleus. It is appropriate for the Secretary of Defense to have these executive agent responsibilities, since the great majority of the effort to accomplish both of these missions is applied to the support of the military aspects of the national security.

The communications security mission is directed at enhancing the security of U.S. Government communications whenever needed to protect those communications from exploitation by foreign governments—a complex undertaking in today's advanced electronic world.

The United States, as part of its effort to produce foreign intelligence, has intercepted foreign communications, analyzed, and in some cases decoded these communications to produce such foreign intelligence since the Revolutionary War. During the Civil War and World War I these communications were often telegrams sent by wire. In modern times, with the advent of wireless communications, particular emphasis has been placed by the Government on the specialized field of intercepting and analyzing communications transmitted by radio. Since the 1930's, elements of the military establishment have been assigned tasks to obtain intelligence from foreign radio transmissions.

In the months preceding Pearl Harbor and throughout World War II, highly successful accomplishments were made by groups in the Army and the Navy to intercept and analyze Japanese and German coded radio messages. Admiral Nimitz is reported as rating its value in the Pacific to the equivalent of another whole fleet. According to another official report, in the victory in the Battle of Midway, it would have been impossible to have achieved the concentration of forces and the tactical surprise without communications intelligence. A congressional committee, in its investigation of Pearl Harbor, stated that the success of communications intelligence "contributed enormously to the defeat of the enemy, greatly shortened the war, and saved many thousands of lives." General George C. Marshall commented that they—communications intelligence—had contributed "greatly to the victories and tremendously to the savings of American lives."

Following World War II, the separate military efforts were brought together and the National Security Agency was formed to focus the Government's efforts. The purpose was to maintain and improve this source of intelligence which was considered of vital importance to the national security, to our ability to wage war, and to the conduct of foreign affairs.

This mission of NSA is directed to foreign intelligence, obtained from foreign electrical communications and also from other foreign signals such as radars. Signals are intercepted by many techniques and processed, sorted, and analyzed by procedures which reject inappropriate or unnecessary signals. The foreign intelligence derived from these signals is then reported to various agencies of the Government in response to their approved requirements for foreign intelligence.

The NSA works very hard at this task, and is composed of dedicated, patriotic citizens, civilian and military, most of whom have dedicated their professional careers to this important and rewarding job. They are justifiably proud of their service to their country and fully accept the fact that their continued remarkable efforts can be appreciated only by those few in Government who know of their great importance to the United States.

Congress, in 1933, recognized the importance of communications intelligence activities and acted to protect the sensitive nature of the information derived from those activities by passing legislation that is now 18 U.S.C. 952. This statute prohibits the divulging of the contents of decoded foreign diplomatic messages, or information about them.

Later, in 1950, Congress enacted 18 U.S.C. 798, which prohibits the unauthorized disclosure, prejudicial use, or publication of classified information of the Government concerning communications intelligence activities, cryptologic activities, or the results thereof. It indicates that the President is authorized: (1) to designate agencies to engage in communications intelligence activities for the United States; (2) to classify cryptologic documents and information; and (3) to determine those persons who shall be given access to sensitive cryptologic documents and information. Further, this law defines the term "communication intelligence" to mean all procedures and methods used in the interception of communications and the obtaining of information from such communications by other than the intended recipients.

After an intensive review by a panel of distinguished citizens, President Truman in 1952 acted to reorganize and strengthen communications intelligence activities. He issued in October 1952 a Presidential memorandum outlining in detail how communications intelligence activities were to be conducted, designated the Secretary of Defense to be his executive agent in these matters, directed the establishment of the NSA, and outlined the missions and functions to be performed by the NSA.

The Secretary of Defense, pursuant to the congressional authority delegated to him in section 133(d) of title 10 of the United States Code, acted to establish the National Security Agency. The section of the law cited provides that the Secretary may exercise any of these duties through persons or organizations of the Department of Defense. In 1962 a Special Subcommittee on Defense Agencies of the House Armed Services Committee concluded, after examining the circumstances leading to the creation of defense agencies, that the Secretary of Defense had the legal authority to establish the National Security Agency.

The President's constitutional and statutory authorities to obtain foreign intelligence through signals intelligence are implemented through National Security Council and Director of Central Intelligence Directives which govern the conduct of signals intelligence activities by the executive branch of the Government.

In 1959, the Congress enacted Public Law 86-36 which provides authority to enable the NSA as the principal agency of the Government responsible for signals intelligence activities, to function without the disclosure of information which would endanger the accomplishment of its functions.

In 1964 Public Law 88-290 was enacted by the Congress to establish a personnel security system and procedures governing persons employed by the NSA or granted access to its sensitive cryptologic information. Public Law 88-290 also delegates authority to the Secretary of Defense to apply these personnel security procedures to employees and persons granted access to the National Security Agency's sensitive information. This law underscores the concern of the Congress regarding the extreme importance of our signals intelligence enterprise and mandates that the Secretary of Defense, and the Director, National Security Agency, take measures to achieve security for the activities of the NSA.

Title 18 U.S.C. 2511(3) provides as follows:

Nothing contained in this chapter or in Section 605 of the Communications Act of 1934, 47 U.S.C. 605, shall limit the constitutional power of the President to take such measures as he deems necessary to protect the nation against actual or potential attack or other hostile acts of a foreign power, to obtain foreign intelligence information deemed essential to the security of the United States, or to protect national security information against foreign intelligence activities.

In *United States v. Brown*, U.S. Court of Appeals, Fifth Circuit, decided August 22, 1973, the court discussed this provision of the law as follows:

The constitutional power of the President is adverted to, although not conferred, by Congress in Title III of the Omnibus Crime Control and Safe Streets Act of 1968.

Thus, while NSA does not look upon section 2511(3) as authority to conduct communications intelligence, it is our position that nothing in chapter 119 of title 18 affects or governs the conduct of communications intelligence for the purpose of gathering foreign intelligence.

Finally, for the past 22 years, Congress has annually appropriated funds for the operation of the NSA, following hearings before the Armed Services and Appropriations Committees of both Houses of Congress in which extensive briefings of the NSA's signals intelligence mission have been conducted. We appear before both the House and the Senate Defense Appropriations Subcommittees to discuss and report on the U.S. signals intelligence and communications security programs, and to justify the budgetary requirements associated with these programs. We do this in formal executive session, in which we discuss our activities in whatever detail required by the Congress.

In considering the fiscal year 1976 total cryptologic budget now before Congress, I appeared before the Defense Subcommittee of the House Appropriations Committee on two separate occasions for approximately 7 hours. In addition, I provided follow-up response to over 100 questions of the subcommittee members and staff. We also appeared before armed services subcommittees concerned with authorizing research, development, test and evaluation, construction and housing programs and also before the appropriations subcommittees on construction and housing.

In addition to this testimony, congressional oversight is accomplished in other ways. Staff members of these subcommittees have periodically visited the Agency for detailed briefings on specific aspects of our operations. Members of the investigations staff of the House Appropriations Committee recently conducted an extensive in-

vestigation of this Agency. The results of this study, which lasted over a year, have been provided to that committee in a detailed report.

Another feature of congressional review is that since 1955 resident auditors of the General Accounting Office have been assigned at the Agency to perform on-site audits. Additional GAO auditors were cleared for access in 1973, and GAO, in addition to this audit, is initiating a classified review of our automatic data processing functions. NSA's cooperative efforts in this area were noted by a Senator in February of this year. In addition, resident auditors of the Office of Secretary of Defense, Comptroller, conduct indepth management reviews of our organization.

A particular aspect of NSA authorities which is pertinent to today's discussion relates to the definition of foreign communications. Neither the Presidential directive of 1952 nor the National Security Council directive No. 6 defines the term foreign communications. The NSA has always confined its activities to communications involving at least one foreign terminal. This interpretation is consistent with the definition of foreign communications in the Communications Act of 1934.

There is also a directive of the Director of Central Intelligence dealing with security regulations which employs a definition which excludes communications between U.S. citizens or entities. While this directive has not been construed as defining the NSA mission in the same sense as has the National Security Council directive, in the past this exclusion has usually been applied and is applied now. However, we will describe a particular activity in the past when that exclusion has not applied.

NSA does not now, and with an exception to be described, has not in the past conducted intercept operations for the purpose of obtaining the communications of U.S. citizens. However, it necessarily occurs that some circuits which are known to carry foreign communications necessary for foreign intelligence will also carry personal communications between U.S. citizens, one of whom is at a foreign location.

The interception of communications, however it may occur, is conducted in such a manner as to minimize the unwanted messages. Nevertheless, many unwanted communications are potentially available for selection. Subsequent processing, sorting, and selecting for analysis is conducted in accordance with strict procedures to insure immediate and, wherever possible, automatic rejection of inappropriate messages. The analysis and reporting is accomplished only for those messages which meet specified conditions and requirements for foreign intelligence. It is certainly believed by NSA that our communications intelligence activities are solely for the purpose of obtaining foreign intelligence in accordance with the authorities delegated by the President stemming from his constitutional power to conduct foreign intelligence.

NSA produces signals intelligence in response to objectives, requirements and priorities as expressed by the Director of Central Intelligence with the advice of the U.S. Intelligence Board. There is a separate committee of the Board which develops the particular requirements against which the NSA is expected to respond.

The principal mechanism used by the Board in formulating requirements for signals intelligence information has been one of listing areas of intelligence interest and specifying in some detail the signals intel-

ligence needed by the various elements of Government. This listing, which was begun in 1966 and fully implemented in 1970, is intended to provide guidance to the Director of the National Security Agency, and to the Secretary of Defense, for programming and operating NSA activities. It is intended as an expression of realistic and essential requirements for signals intelligence information.

This process recognizes that a single listing, updated annually, needs to be supplemented with additional detail and time-sensitive factors, and it establishes a procedure whereby the USIB agencies can express directly to the NSA information needs which reasonably amplify requirements approved by USIB or higher authority.

In addition, there are established procedures for non-Board members, the Secret Service, and the BNDD at the time in question, to ask the NSA for information. The NSA does have operational discretion in responding to requirements, but we do not generate our own requirements for foreign intelligence. The Director, NSA is directed to be responsive to the requirements formulated by the Director of Central Intelligence. However, I clearly must not respond to any requirements which I feel are not proper.

In 1975 the USIB signals intelligence requirements process was revised. Under the new system, all basic requirements for signals intelligence information on U.S. Government agencies will be reviewed and validated by the Signals Intelligence Committee of USIB before being levied on the NSA. An exception is those requirements which are highly time-sensitive; they will continue to be passed simultaneously to us for action and to USIB for information. The new system will also attempt to prioritize signals intelligence requirements. The new requirements process is an improvement in that it creates a formal mechanism to record all requirements for signals intelligence information and to establish their relative priorities.

Now to the subject which the committee asked me to address in some detail—the so-called watch list activity of 1967 to 1973.

The use of lists of words, including individual names, subjects, locations, et cetera, has long been one of the methods used to sort out information of foreign intelligence value from that which is not of interest. In the past such lists have been referred to occasionally as watch lists, because the lists were used as an aid to watch for foreign activity of reportable intelligence interest. However, these lists generally did not contain names of U.S. citizens or organizations. The activity in question is one in which U.S. names were used systematically as a basis for selecting messages, including some between U.S. citizens, when one of the communicants was at a foreign location.

The origin of such activity is unclear. During the early sixties, requesting agencies had asked the NSA to look for reflections in international communications of certain U.S. citizens traveling to Cuba. Beginning in 1967, requesting agencies provided names of persons and organizations, some of whom were U.S. citizens, to the NSA in an effort to obtain information which was available in foreign communications as a by-product of our normal foreign intelligence mission.

The purpose of the lists varied, but all possessed a common thread in which the NSA was requested to review information available through our usual intercept sources. The initial purpose was to help determine the existence of foreign influence on specified activities of

interest to agencies of the U.S. Government, with emphasis then on Presidential protection and on civil disturbances occurring throughout the Nation.

Later, because of other developments, such as widespread national concern over such criminal activity as drug trafficking and acts of terrorism, both domestic and international, the emphasis came to include these areas. Thus, during this period, 1967-73, requirements for which lists were developed in four basic areas: international drug trafficking; Presidential protection; acts of terrorism; and possible foreign support or influence on civil disturbances.

In the sixties there was Presidential concern voiced over the massive flow of drugs into our country from outside the United States. Early in President Nixon's administration, he instructed the CIA to pursue with vigor intelligence efforts to identify foreign sources of drugs and the foreign organizations and methods used to introduce illicit drugs into the United States. The BNDD, the Bureau of Narcotics and Dangerous Drugs, in 1970 asked the NSA to provide communications intelligence relevant to these foreign aspects, and BNDD provided watch lists with some U.S. names [exhibit 4].<sup>1</sup> International drug trafficking requirements were formally documented in USIB requirements in August 1971.

As we all know, during this period there was also heightened concern by the country and the Secret Service over Presidential protection because of President Kennedy's assassination. After the Warren Report, requirements lists containing names of U.S. citizens and organizations were provided to NSA by the Secret Service in support of their efforts to protect the President and other senior officials. Such requirements were later incorporated into USIB documentation. At that time, intelligence derived from foreign communications was regarded as a valuable tool in support of Executive protection.

About the same time as the concern over drugs, or shortly thereafter, there was a committee established by the President to combat international terrorism. This committee was supported by an inter-departmental working group with USIB representatives. Requirements to support this effort with communications intelligence were also incorporated into USIB documentation.

Now let me put the watch list in perspective regarding its size and the numbers of names submitted by the various agencies:

The BNDD submitted a watch list covering their requirements for intelligence on international narcotics trafficking. On September 8, 1972, President Nixon summarized the efforts of his administration against drug abuse. The President stated that he ordered the Central Intelligence Agency, early in his administration, to mobilize its full resources to fight the international drug trade. The key priority, the President noted, was to destroy the trafficking through law enforcement and intelligence efforts. The BNDD list contained the names of suspected drug traffickers. There were about 450 U.S. individuals and over 3,000 foreign individuals.

The Secret Service submitted watch lists covering their requirements for intelligence relating to Presidential and Executive protec-

---

<sup>1</sup> See p. 151.

tion. Public Law 90-331 of June 6, 1968, made it mandatory for Federal agencies to assist the Secret Service in the performance of its protective duties. These lists contained names of persons and groups who, in the opinion of the Secret Service, were potentially a threat to Secret Service protectees, as well as the names of the protectees themselves. On these lists were about 180 U.S. individuals and groups and about 525 foreign individuals and groups.

An Army message of October 20, 1967, informed the NSA that Army ACSI, assistant chief of staff for intelligence, had been designated executive agent by DOD for civil disturbance matters and requested any available information on foreign influence over, or control of, civil disturbances in the U.S. [exhibit 1].<sup>1</sup> The Director, NSA, sent a cable the same day to the DCI and to each USIB member and notified them of the urgent request from the Army and stated that the NSA would attempt to obtain communications intelligence regarding foreign control or influence over certain U.S. individuals and groups [exhibit 2].<sup>2</sup>

The Brownell Committee, whose report led to the creation of NSA, stated that communications intelligence should be provided to the Federal Bureau of Investigation because of the essential role of the Bureau in the national security.

The FBI submitted watch lists covering their requirements on foreign ties and support to certain U.S. persons and groups. These lists contained names of "so-called" extremist persons and groups, individuals and groups active in civil disturbances, and terrorists. The lists contained a maximum of about 1,000 U.S. persons and groups and about 1,700 foreign persons and groups.

The DIA submitted a watch list covering their requirements on possible foreign control of, or influence on, U.S. antiwar activity. The list contained names of individuals traveling to North Vietnam. There were about 20 U.S. individuals on this list. DIA is responsible under DOD directives for satisfying the intelligence requirements of the major components of the DOD and to validate and assign to NSA requirements for intelligence required by DOD components.

Between 1967 and 1973 there was a cumulative total of about 450 U.S. names on the narcotics list, and about 1,200 U.S. names on all other lists combined. What that amounted to was that at the height of the watch list activity, there were about 800 U.S. names on the watch list and about one-third of these 800 were from the narcotics list.

We estimate that over this 6-year period, 1967-1973, about 2,000 reports were issued by the NSA on international narcotics trafficking, and about 1,900 reports were issued covering the three areas of terrorism, Executive protection and foreign influence over U.S. groups. This would average about two reports per day. These reports included some messages between U.S. citizens with one foreign communicant, but over 90 percent had at least one foreign communicant and all messages had at least one foreign terminal. Using agencies did periodically review, and were asked by the NSA to review, their watch lists to insure inappropriate or unnecessary entries were promptly removed.

I am not the proper person to ask concerning the value of the product from these four special efforts. We are aware that a major terrorist

---

<sup>1</sup> See p. 145.  
<sup>2</sup> See p. 147.

act in the United States was prevented. In addition, some large drug shipments were prevented from entering the United States because of our efforts on international narcotics trafficking. We have statements from the requesting agencies in which they have expressed appreciation for the value of the information which they had received from us. Nonetheless, in my own judgment, the controls which were placed on the handling of the intelligence were so restrictive that the value was significantly diminished.

Now let me address the question of the watch list activity as the NSA saw it at the time.

This activity was reviewed by proper authority within NSA and by competent external authority. This included two former Attorneys General and a former Secretary of Defense.

The requirements for information had been approved by officials of the using agencies and subsequently validated by the United States Intelligence Board. For example, the Secret Service and BNDD requirements were formally included in USIB guidance in 1970 and 1971, respectively.

In the areas of narcotics trafficking, terrorism and requirements related to the protection of the lives of senior U.S. officials, the emphasis placed by the President on a strong, coordinated Government effort was clearly understood. There also was no question that there was considerable Presidential concern and interest in determining the existence and extent of foreign support to groups fomenting civil disturbances in the United States.

From 1967 to 1969 the procedure for submitting names was more informal, with written requests following as the usual practice. Starting in 1969 the procedure was formalized and the names for watch lists were submitted through channels in writing [exhibit 3].<sup>1</sup> The Director and Deputy Director of the NSA approved certain categories of subject matter from customer agencies, and were aware that U.S. individuals and organizations were being included on watch lists. While they did not review and approve each individual name, there were continuing management reviews at levels below the Directorate.

NSA personnel sometimes made analytic amplifications on customer watch list submissions in order to fulfill certain requirements. For example, when information was received that a name on the watch list used an alias, the alias was inserted; or when an address was uncovered of a watch list name, the address was included. This practice by analysts was done to enhance the selection process, not to expand the lists.

The information produced by the watch list activity was, with one exception, entirely a byproduct of our foreign intelligence mission. All collection was conducted against international communications with at least one terminal in a foreign country, and for purposes unrelated to the watch list activity. That is, the communications were obtained, for example, by monitoring communications to and from Hanoi.

All communications had a foreign terminal and the foreign terminal or communicant, with the one exception to be described, was the initial object of the communications collection.

The watch list activity specifically consisted of scanning international communications already intercepted for other purposes to derive

---

<sup>1</sup> See p. 149.

information which met watch list requirements. This scanning was accomplished by using the entries provided to NSA as selection criteria. Once selected, the messages were analyzed to determine if the information therein met those requesting agencies' requirements associated with the watch lists. If the message met the requirement, the information therein was reported to the requesting agency in writing.

Now let me discuss for a moment the manner in which intelligence derived from the watch lists was handled.

For the period 1967-69, international messages between U.S. citizens and organizations, selected on the basis of watch list entries and containing foreign intelligence, were issued for background use only and were hand delivered to certain requesting agencies. If the U.S. citizen or organization was only one correspondent of the international communication, it was published as a normal product report but in a special series to limit distribution on a strict need-to-know basis.

Starting in 1969, any messages that fell into the categories of Presidential/executive protection and foreign influence over U.S. citizens and groups were treated in an even more restricted fashion. They were provided for background use only and hand delivered to requesting agencies. When the requirements to supply intelligence regarding international drug trafficking in 1970 and international terrorism in 1971 were received, intelligence on these subjects was handled in a similar manner. This procedure continued until I terminated the activity in 1973.

The one instance in which foreign messages were intercepted for specific watch list purposes was the collection of some telephone calls passed over international communications facilities between the United States and South America. The collection was conducted at the specific request of the BNDD to produce intelligence information on the methods and locations of foreign narcotics trafficking.

In addition to our own intercept, CIA was asked by NSA to assist in this collection. NSA provided to CIA names of individuals from the international narcotics trafficking watch list. This collection by CIA lasted for approximately 6 months, from late 1972 to early 1973, when CIA stopped because of concern that the activity exceeded CIA statutory restrictions.

When the watch list activity began, the NSA and others viewed the effort as an appropriate part of the foreign intelligence mission. The emphasis of the President that a concerted national effort was required to combat these grave problems was clearly expressed.

The activity was known to higher authorities, kept quite secret, and restrictive controls were placed on the use of the intelligence. The agencies receiving the information were clearly instructed that the information could not be used for prosecutive or evidentiary purposes, and to our knowledge, it was not used for such purposes.

It is worth noting that some Government agencies receiving the information had dual functions. For instance, BNDD was concerned on the one hand with domestic drug law enforcement activities and on the other hand with the curtailing of international narcotics trafficking. It would be to the latter area of responsibility that the NSA delivered its intelligence.

However, since the intelligence was being reported to some agencies which did have law enforcement responsibilities, there was growing

concern that the intelligence could be used for purposes other than foreign intelligence. To minimize this risk, the material was delivered only to designated offices in those agencies, and the material was marked and protected in a special way to limit the number of people involved and to segregate it from information of broader interest.

In 1973, concern about the NSA's role in these activities was increased, first, by concerns that it might not be possible to distinguish definitely between the purpose for the intelligence gathering which NSA understood was served by these requirements, and the missions and functions of the departments or agencies receiving the information, and, second, that requirements from such agencies were growing, and finally, that new broad discovery procedures in court cases were coming into use which might lead to disclosure of sensitive intelligence sources and methods.

The first action taken was the decision to terminate the activity in support of BNDD in the summer of 1973. This decision was made because of concern that it might not be possible to make a clear separation between the requests for information submitted by BNDD as it pertained to legitimate foreign intelligence requirements and the law-enforcement responsibility of BNDD.

CIA had determined in 1973 that it could not support these requests of BNDD because of statutory restrictions on CIA. The NSA is not subject to the same sort of restrictions as CIA, but a review of the matter led to a decision that certain aspects of our support should be discontinued, and in particular the watch-list activity was stopped.

NSA did not retain any of the BNDD watch lists or product. It was destroyed in the fall of 1973, since there seemed no purpose or requirement to retain it.

With regard to watch lists submitted by FBI, CIA, and Secret Service, these matters were discussed with the National Security Agency Counsel and Counsel for the Department of Defense, and we stopped the distribution of information in the summer of 1973. In September 1973, I sent a letter to each agency head requesting him to recertify the requirement with respect to the appropriateness of the request, including a review of that agency's legal authorities [exhibit 6].<sup>1</sup>

Somewhat later, on October 1, 1973, Attorney General Richardson wrote me, indicating that he was concerned with respect to the propriety of requests for information concerning U.S. citizens which NSA had received from the FBI and Secret Service [exhibit 7].<sup>2</sup> He wrote the following:

Until I am able more carefully to assess the effect of *Keith* and other Supreme Court decisions concerning electronic surveillance upon your current practice of disseminating to the FBI and Secret Service information acquired by you through electronic devices pursuant to requests from the FBI and Secret Service, it is requested that you immediately curtail the further dissemination of such information to these agencies.

He goes on to say:

Of course, relevant information acquired by you in the routine pursuit of the collection of foreign intelligence may continue to be furnished to appropriate government agencies.

---

<sup>1</sup> See p. 158.

<sup>2</sup> See p. 160.

The overall result of these actions was that we stopped accepting watch lists containing names of U.S. citizens and no information is produced or disseminated to other agencies using these methods [exhibit 8].<sup>1</sup> Thus, the watch list activity which involved U.S. citizens ceased operationally in the summer of 1973 and was terminated officially in the fall of 1973.

As to the future, the Attorney General's direction is that we may not accept any requirement based on the names of U.S. citizens unless he has personally approved such a requirement; and no such approval has been given. Additionally, directives now in effect in various agencies, including NSA, also preclude the resumption of such activity.

[The full statement of Lt. Gen. Lew Allen, Jr. follows:]

**PREPARED STATEMENT OF LT. GEN. LEW ALLEN, JR., DIRECTOR, NATIONAL SECURITY AGENCY**

Mr. Chairman Members of the Committee, I recognize the important responsibility this Committee has to investigate the intelligence operations of the United States Government and to determine the need for improvement by legislative or other means. For several months, involving many thousands of manhours, the National Security Agency has, I believe, cooperated with this Committee to provide a thorough information base, including data whose continued secrecy is most important to our nation.

I am now here to discuss in open session certain aspects of an important and hitherto secret operation of the U.S. Government. I recognize that the Committee is deeply concerned that we protect sensitive and fragile sources of information. I appreciate the care which this Committee and Staff have exercised to protect the sensitive data we have provided. I also understand that the Committee intends to restrict this open discussion to certain specified activities and to avoid current foreign intelligence operations. It may not be possible to discuss all these activities completely without some risk of damage to continuing foreign intelligence capabilities. Therefore, I may request some aspects of our discussion be conducted in executive session where there can be opportunity to continue our full and frank disclosure to the Committee of all information required. The Committee may then develop an appropriate public statement. We are therefore here, sir, at your request, prepared to cooperate in bringing these matters before your Committee.

**WHAT I PROPOSE TO COVER**

In the interest of clarity and perspective, I shall first review the purpose of the National Security Agency and the authorities under which it operates. Next, I will describe the process by which requirements for information are levied on NSA by other government agencies. And finally, I will give a more specific description of an operation conducted in 1967-1973 by NSA in response to external requirements, which I will refer to as "the watch list activity." This activity has been subject to an intensive review by this Committee and Staff in closed session.

**NSA'S MISSION**

Under the authority of the President, the Secretary of Defense has been delegated responsibility for both providing security of U.S. governmental communications and seeking intelligence from foreign electrical communications. Both functions are executed for the Secretary of Defense by the Director, National Security Agency, through a complex national system which includes the National Security Agency at its nucleus.

It is appropriate for the Secretary of Defense to have these executive agent responsibilities, since the great majority of the effort to accomplish both of these missions is applied to the support of the military aspects of the national security.

---

<sup>1</sup> See p. 162.

The Communications Security mission is directed at enhancing the security of U.S. Government communications whenever needed to protect the communications from exploitation by foreign governments—a complex undertaking in today's advanced electronic world.

The United States, as part of its effort to produce foreign intelligence, has intercepted foreign communications, analyzed, and in some cases decoded, these communications to produce such foreign intelligence since the Revolutionary War. During the Civil War and World War I these communications were often telegrams sent by wire.

In modern times, with the advent of wireless communications, particular emphasis has been placed by the government on the specialized field of intercepting and analyzing communications transmitted by radio. Since the 1930's, elements of the military establishment have been assigned tasks to obtain intelligence from foreign radio transmissions. In the months preceding Pearl Harbor and throughout World War II, highly successful accomplishments were made by groups in the Army and the Navy to intercept and analyze Japanese and German coded radio messages. Admiral Nimitz is reported as rating its value in the Pacific to the equivalent of another whole fleet; General Handy is reported to have said that it shortened the war in Europe by at least a year. According to another official report, in the victory in the Battle of Midway, it would have been impossible to have achieved the concentration of forces and the tactical surprise without communications intelligence. It also contributed to the success of the Normandy invasion. Both the Army and Navy obtained invaluable intelligence from the enciphered radio messages in both Europe and the Pacific. A Congressional committee, in its investigation of Pearl Harbor, stated that the success of communications intelligence "contributed enormously to the defeat of the enemy, greatly shortened the war, and saved many thousands of lives." General George C. Marshall, referring to similar activities during World War II, commented that they had contributed "greatly to the victories and tremendously to the savings of American lives." Similar themes run through the writings of many U.S. military officers and policy officials from that period and subsequently in our more recent history. Following World War II, the separate military efforts were brought together and the National Security Agency was formed to focus the government's efforts. The purpose was to maintain and improve this source of intelligence which was considered of vital importance to the national security, to our ability to wage war, and to the conduct of foreign affairs.

This mission of NSA is directed to foreign intelligence, obtained from foreign electrical communications and also from other foreign signals such as radars. Signals are intercepted by many techniques and processed, sorted and analyzed by procedures which reject inappropriate or unnecessary signals. The foreign intelligence derived from these signals is then reported to various agencies of the government in response to their approved requirements for foreign intelligence. The National Security Agency works very hard at this task, and is composed of dedicated, patriotic citizens, civilian and military, most of whom have dedicated their professional careers to this important and rewarding job. They are justifiably proud of their service to their country and fully accept the fact that their continued remarkable efforts can be appreciated only by those few in government who know of their great importance to the U.S.

#### NSA AUTHORITIES

Congress, in 1933, recognized the importance of communications intelligence activities and acted to protect the sensitive nature of the information derived from those activities by passing legislation that is now 18 U.S.C. 952. This statute prohibits the divulging of the contents of decoded foreign diplomatic messages, or information about them.

Later, in 1950, Congress enacted 18 U.S.C. 798, which prohibits the unauthorized disclosure, prejudicial use, or publication of classified information of the Government concerning communications intelligence activities, cryptologic activities, or the results thereof. It indicates that the President is authorized: (1) To designate agencies to engage in communications intelligence activities for the United States. (2) to classify cryptologic documents and information, and (3) to determine those persons who shall be given access to sensitive cryptologic documents and information. Further, this law defines the term "communication intelligence" to mean all procedures and methods used in the interception of

communications and the obtaining of information from such communications by other than the intended recipients.

After an intensive review by a panel of distinguished citizens, President Truman in 1952 acted to reorganize and strengthen communications intelligence activities. He issued in October 1952 a Presidential memorandum outlining in detail how communications intelligence activities were to be conducted, designated the Secretary of Defense to be his executive agent in these matters, directed the establishment of the National Security Agency, and outlined the missions and functions to be performed by the National Security Agency.

The Secretary of Defense, pursuant to the Congressional authority delegated him in Section 133(d) of Title 10 of the U.S. Code, acted to establish the National Security Agency. The section of the law cited provides that the Secretary may exercise any of these duties through persons or organizations of the Department of Defense. In 1962 a Special Subcommittee on Defense Agencies of the House Armed Services Committee concluded, after examining the circumstances leading to the creation of defense agencies, that the Secretary of Defense had the legal authority to establish the National Security Agency.

The President's constitutional and statutory authorities to obtain foreign intelligence through signals intelligence are implemented through National Security Council and Director of Central Intelligence directives which govern the conduct of signals intelligence activities by the Executive branch of the government.

In 1959, the Congress enacted Public Law 86-36 which provides authority to enable the National Security Agency, as the principal agency of the government responsible for signals intelligence activities, to function without the disclosure of information which would endanger the accomplishment of its functions.

In 1964 Public Law 88-290 was enacted by the Congress to establish a personnel security system and procedures governing persons employed by the National Security Agency or granted access to its sensitive cryptologic information. Public Law 88-290 also delegates authority to the Secretary of Defense to apply these personnel security procedures to employees and persons granted access to the National Security Agency's sensitive information. This law underscores the concern of the Congress regarding the extreme importance of our signals intelligence enterprise and mandates that the Secretary of Defense, and the Director, National Security Agency, take measures to achieve security for the activities of the National Security Agency.

Title 18 U.S.C. 2511(3) provides as follows: "Nothing contained in this chapter or in Section 605 of the Communications Act of 1934 (47 U.S.C. 605) shall limit the constitutional power of the President to take such measures as he deems necessary to protect the nation against actual or potential attack or other hostile acts of a foreign power, to obtain foreign intelligence information deemed essential to the security of the United States, or to protect national security information against foreign intelligence activities. . . ."

In *United States v. Brown*, United States Court of Appeals, Fifth Circuit, decided 22 August 1973, the Court discussed this provision of the law as follows:

"The constitutional power of the President is adverted to, although not conferred, by Congress in Title III of the Omnibus Crime Control and Safe Streets Act of 1968."

Thus, while NSA does not look upon Section 2511(3) as authority to conduct communications intelligence, it is our position that nothing in Chapter 119 of Title 18 affects or governs the conduct of communications intelligence for the purpose of gathering foreign intelligence.

Finally, for the past 22 years, Congress has annually appropriated funds for the operation of the National Security Agency, following hearings before the Armed Services and Appropriations Committees of both Houses of Congress in which extensive briefings of the National Security Agency's signals intelligence mission have been conducted.

We appear before both the House and the Senate Defense Appropriations Subcommittees to discuss and report on the U.S. signals intelligence and communications security programs, and to justify the budgetary requirements associated with these programs. We do this in formal executive session, in which we discuss our activities in whatever detail required by the Congress. In considering the Fiscal Year '76 total cryptologic budget now before Congress, I appeared before the Defense Subcommittee of the House Appropriations Committee on two separate occasions for approximately seven hours. In addition, I provided follow-up response to over one hundred questions of the Subcommittee

members and staff. We also appeared before Armed Services Subcommittees concerned with authorizing research, development, test and evaluation (RDT&E), construction and housing programs and also before the Appropriations Subcommittees on construction and housing.

In addition to this testimony, Congressional oversight is accomplished in other ways. Staff members of these subcommittees have periodically visited the Agency for detailed briefings on specific aspects of our operations. Members of the investigations staff of the House Appropriations Committee recently conducted an extensive investigation of this Agency. The results of this study, which lasted over a year, have been provided to that committee in a detailed report.

Another feature of Congressional review is that since 1955 resident auditors of the General Accounting Office have been assigned at the Agency to perform on-site audits. Additional GAO auditors were cleared for access in 1973 and GAO, in addition to this audit, is initiating a classified review of our automatic data processing functions. NSA's cooperative efforts in this area were noted by a Senator in February of this year.

In addition, resident auditors of the Office of Secretary of Defense, Comptroller, conduct in depth management reviews of our organization.

A particular aspect of NSA authorities which is pertinent to today's discussion relates to the definition of foreign communications. Neither the Presidential Directive of 1952 nor the National Security Council Directive No. 6 defines the term foreign communications. The National Security Agency has always confined its activities to communications involving at least one foreign terminal. This interpretation is consistent with the definition of foreign communications in the Communications Act of 1934. There is also a Directive of the Director of Central Intelligence dealing with security regulations which employs a definition which excludes communications between U.S. citizens or entities. While this Directive has not been construed as defining the NSA mission in the same sense as has the National Security Council Directive, in the past this exclusion has usually been applied and is applied now. However, we will describe a particular activity in the past when that exclusion was not applied. NSA does not now, and with an exception to be described, has not in the past conducted intercept operations for the purpose of obtaining the communications of U.S. citizens. However, it necessarily occurs that some circuits which are known to carry foreign communications necessary for foreign intelligence will also carry personal communications between U.S. citizens, one of whom is at a foreign location. The interception of communications, however it may occur, is conducted in such a manner as to minimize the unwanted messages. Nevertheless, many unwanted communications are potentially available for selection. Subsequent processing, sorting and selecting for analysis, is conducted in accordance with strict procedures to insure immediate and, where possible, automatic rejection of inappropriate messages. The analysis and reporting is accomplished only for those messages which meet specified conditions and requirements for foreign intelligence. It is certainly believed by NSA that our communications intelligence activities are solely for the purpose of obtaining foreign intelligence in accordance with the authorities delegated by the President stemming from his constitutional power to conduct foreign intelligence.

#### OVERALL REQUIREMENTS ON NSA

NSA produces signals intelligence in response to objectives, requirements, and priorities as expressed by the Director of Central Intelligence with the advice of the United States Intelligence Board. There is a separate committee of the Board which develops the particular requirements against which the National Security Agency is expected to respond.

The principal mechanism used by the Board in formulating requirements for signals intelligence information has been one of listing areas of intelligence interest and specifying in some detail the signals intelligence needed by the various elements of government. This listing which was begun in 1966 and fully implemented in 1970, is intended to provide guidance to the Director of the National Security Agency (and to the Secretary of Defense) for programming and operating National Security Agency activities. It is intended as an expression of realistic and essential requirements for signals intelligence information. This process recognizes that a single listing, updated annually needs to be supplemented with additional detail and time-sensitive factors and it establishes a procedure whereby the USIB agencies can express, directly to the National Se-

curity Agency, information needs which reasonably amplify requirements approved by USIB or higher authority. In addition, there are established procedures for non-Board members (the Secret Service and the BNDD at the time) to task the National Security Agency for information. The National Security Agency does have operational discretion in responding to requirements but we do not generate our own requirements for foreign intelligence. The Director, NSA is directed to be responsive to the requirements formulated by the Director of Central Intelligence, however, I clearly must not respond to any requirements which I feel are not proper.

In 1975 the USIB signals intelligence requirements process was revised. Under the new system, all basic requirements for signals intelligence information on United States Government agencies will be reviewed and validated by the Signals Intelligence Committee of USIB before being levied on the National Security Agency. An exception is those requirements which are highly time-sensitive; they will continue to be passed simultaneously to us for action and to USIB for information. The new system will also attempt to prioritize signals intelligence requirements. The new requirements process is an improvement in that it creates a formal mechanism to record all requirements for signals intelligence information and to establish their relative priorities.

#### THE WATCH LIST

Now to the subject which the Committee asked me to address in some detail—the so-called watch list activity of 1967-1973.

The use of lists of words, including individual names, subjects, locations, etc, has long been one of the methods used to sort out information of foreign intelligence value from that which is not of interest. In the past such lists have been referred to occasionally as "watch lists," because the lists were used as an aid to watch for foreign activity of reportable intelligence interest. However, these lists generally did not contain names of U.S. citizens or organizations. The activity in question is one in which U.S. names were used systematically as a basis for selecting messages, including some between U.S. citizens when one of the communicants was at a foreign location.

The origin of such activity is unclear. During the early '60's, requesting agencies had asked the National Security Agency to look for reflections in international communications of certain U.S. citizens travelling to Cuba. Beginning in 1967, requesting agencies provided names of persons and organizations (some of whom were U.S. citizens) to the National Security Agency in an effort to obtain information which was available in foreign communications as a by-product of our normal foreign intelligence mission. The purpose of the lists varied, but all possessed a common thread in which the National Security Agency was requested to review information available through our usual intercept sources. The initial purpose was to help determine the existence of foreign influence on specified activities of interest to agencies of the U.S. Government, with emphasis on presidential protection and on civil disturbances occurring throughout the nation. Later, because of other developments, such as widespread national concern over such criminal activity as drug trafficking and acts of terrorism, both domestic and international, the emphasis came to include these areas. Thus, during this period, 1967-1973, requirements for watch lists were developed in four basic areas: international drug trafficking, Presidential protection, acts of terrorism, and possible foreign support or influence on civil disturbances.

In the '60's, there was Presidential concern voiced over the massive flow of drugs into our country from outside the United States. Early in President Nixon's administration, he instructed the CIA to pursue with vigor, intelligence efforts to identify foreign sources of drugs and the foreign organizations and methods used to introduce illicit drugs into the U.S. The BNDD in 1970 asked the National Security Agency to provide communications intelligence relevant to these foreign aspects and BNDD provided watch lists with some U.S. names. International drug trafficking requirements were formally documented in USIB requirements in August 1971.

As we all know, during this period there was also heightened concern by the country and the Secret Service over Presidential protection because of President Kennedy's assassination. After the Warren Report, requirements lists containing names of U.S. citizens and organizations were provided to NSA by the Secret Service in support of their efforts to protect the President and other senior officials. Such requirements were later incorporated into USIB documentation. At

that time intelligence derived from foreign communications was regarded as a valuable tool in support of executive protection.

About the same time as the concern over drugs, or shortly thereafter, there was a committee established by the President to combat international terrorism. This committee was supported by a working group from the USIB. Requirements to support this effort with communications intelligence were also incorporated into USIB documentation.

Now let me put the "watch list" in perspective regarding its size and the numbers of names submitted by the various agencies:

The BNDD submitted a "watch list" covering their requirements for intelligence on international narcotics trafficking. On September 8, 1972, President Nixon summarized the efforts of his administration against drug abuse. The President stated that he ordered the Central Intelligence Agency, early in his administration, to mobilize its full resources to fight the international drug trade. The key priority, the President noted, was to destroy the trafficking through law enforcement and intelligence efforts. The BNDD list contained names of suspected drug traffickers. There were about 450 U.S. individuals and over 3,000 foreign individuals.

The Secret Service submitted "watch lists" covering their requirements for intelligence relating to Presidential and Executive protection. Public Law 90-381 of June 6, 1968, made it mandatory for Federal agencies to assist the Secret Service in the performance of its protective duties. These lists contained names of persons and groups who in the opinion of the Secret Service were potentially a threat to Secret Service protectees, as well as the names of the protectees themselves. On these lists were about 180 U.S. individuals and groups and about 525 foreign individuals and groups.

An Army message of 20 October 1967 informed the National Security Agency that Army ACSI had been designated executive agent by DoD for civil disturbance matters and requested any available information on foreign influence over, or control of, civil disturbances in the U.S. The Director, National Security Agency sent a cable the same day to the DCI and to each USIB member and notified them of the urgent request from the Army and stated that the National Security Agency would attempt to obtain COMINT regarding foreign control or influence over certain U.S. individuals and groups.

The Brownell Committee, whose report led to the creation of NSA, stated that communications intelligence should be provided to the Federal Bureau of Investigation because of the essential role of the Bureau in the national security.

The FBI submitted "watch lists" covering their requirements on foreign ties and support to certain U.S. persons and groups. These lists contained names of "so-called" extremist persons and groups, individuals and groups active in civil disturbances, and terrorists. The lists contained a maximum of about 1,000 U.S. persons and groups and about 1,700 foreign persons and groups.

The CIA submitted "watch lists" covering their requirements on international travel, foreign influence and foreign support of "so-called" U.S. extremists and terrorists. Section 403(d)(3) of Title 50, U.S. Code, provided that it was the duty of the Central Intelligence Agency to correlate and evaluate intelligence relating to the national security and to provide for the appropriate dissemination of such intelligence within the government using, where appropriate, existing agencies and facilities. These lists contained about 30 U.S. individuals and about 700 foreign individuals and groups.

The DIA submitted a "watch list" covering their requirements on possible foreign control of, or influence on, U.S. anti-war activity. The list contained names of individuals traveling to North Vietnam. There were about 20 U.S. individuals on this list. DIA is responsible under DoD directives for satisfying the intelligence requirements of the major components of the DoD and to validate and assign to NSA requirements for intelligence required by DoD components.

Between 1967 and 1973 there was a cumulative total of about 450 U.S. names on the narcotics list, and about 1,200 U.S. names on all other lists combined. What that amounted to was that at the height of the watch list activity, there were about 800 U.S. names on the "watch list" and about one third of this 800 were from the narcotics list.

We estimate that over this six year period (1967-1973) about 2,000 reports were issued by the National Security Agency on international narcotics trafficking, and about 1,900 reports were issued covering the three areas of terrorism, executive protection and foreign influence over U.S. groups. This would average about two reports per day. These reports included some messages between U.S.

citizens, but over 90% had at least one foreign communicant and all messages had at least one foreign terminal. Using agencies did periodically review (and were asked by the National Security Agency to review) their "watch lists" to ensure inappropriate or unnecessary entries were promptly removed. I am not the proper person to ask concerning the value of the product from these four special efforts. We are aware that a major terrorist act in the U.S. was prevented. In addition, some large drug shipments were prevented from entering the U.S. because of our efforts on international narcotics trafficking. We have statements from the requesting agencies in which they have expressed appreciation for the value of the information which they had received from us. Nonetheless, in my own judgment, the controls which were placed on the handling of the intelligence were so restrictive that the value was significantly diminished.

Now let me address the question of the "watch list" activity as the National Security Agency saw it at the time. This activity was reviewed by proper authority within National Security Agency and by competent external authority. This included two former Attorneys General and a former Secretary of Defense. The requirements for information had also been approved by officials of the using agencies and subsequently validated by the United States Intelligence Board. For example, the Secret Service and BNDD requirements were formally included in USIB guidance in 1970 and 1971, respectively. In the areas of narcotics trafficking, terrorism, and requirements related to the protection of the lives of senior U.S. officials, the emphasis placed by the President on a strong, coordinated government effort was clearly understood. There also was no question that there was considerable Presidential concern and interest in determining the existence and extent of foreign support to groups fomenting civil disturbances in the United States.

From 1967-1969 the procedure for submitting names was more informal with written requests following as the usual practice. Starting in 1969 the procedure was formalized and the names for "watch lists" were submitted through channels in writing. The Director and Deputy Director of the National Security Agency approved certain categories of subject matter from customer agencies, and were aware that U.S. individuals and organizations were being included on "watch lists." While they did not review and approve each individual name, there were continuing management reviews at levels below the Directorate. National Security Agency personnel sometimes made analytic amplifications on customer "watch list" submissions in order to fulfill certain requirements. For example, when information was received that a name on the "watch list" used an alias, the alias was inserted; or when an address was uncovered of a "watch list" name, the address was included. This practice by analysts was done to enhance the selection process, not to expand the lists.

The information produced by the "watch list" activity was, with one exception, entirely a by-product of our foreign intelligence mission. All collection was conducted against international communications with at least one terminal in a foreign country, and for purposes unrelated to the "watch list" activity. That is, the communications were obtained, for example, by monitoring communications to and from Hanoi. All communications had a foreign terminal and the foreign terminal or communicant (with the one exception) was the initial object of the communications collection. The "watch list" activity itself specifically consisted of scanning international communications already intercepted for other purposes to derive information which met "watch list" requirements. This scanning was accomplished by using the entries provided to NSA as selection criteria. Once selected, the messages were analyzed to determine if the information therein met those requesting agencies' requirements associated with the "watch lists." If the message met the requirement, the information therein was reported to the requesting agency in writing.

Now let me discuss for a moment the manner in which intelligence derived from the "watch lists" was handled. For the period 1967-1969, international messages between U.S. citizens and organizations, selected on the basis of "watch list" entries and containing foreign intelligence, were issued for background use only and were hand-delivered to certain requesting agencies. If the U.S. citizen or organization was only one correspondent of the international communication, it was published as a normal product report but in a special series to limit distribution on a strict need-to-know basis.

Starting in 1969, any messages that fell into the categories of Presidential/executive protection and foreign influence over U.S. citizens and groups were treated in an even more restricted fashion. They were provided for background

use only and hand-delivered to requesting agencies. When the requirements to supply intelligence regarding international drug trafficking in 1970 and international terrorism in 1971 were received, intelligence on these subjects was handled in a similar manner. This procedure continued until I terminated the activity in 1973.

The one instance in which foreign messages were intercepted for specific "watch list" purposes was the collection of some telephone calls passed over international communications facilities between the United States and South America. The collection was conducted at the specific request of the BNDD to produce intelligence information on the methods and locations of foreign narcotics trafficking. In addition to our own intercept, CIA was asked by NSA to assist in this collection. NSA provided to CIA names of individuals from the international narcotics trafficking watch list. This collection by CIA lasted for approximately six months, from late 1972 to early 1973, when CIA stopped because of concern that the activity exceeded CIA statutory restrictions.

When the "watch list" activity began, the National Security Agency and others viewed the effort as an appropriate part of the foreign intelligence mission. The emphasis of the President that a concerted national effort was required to combat these grave problems was clearly expressed. The activity was known to higher authorities, kept quite secret, and restrictive controls were placed on the use of the intelligence. The agencies receiving the information were clearly instructed that the information could not be used for prosecutive or evidentiary purposes and to our knowledge it was not used for such purposes.

It is worth noting that some government agencies receiving the information had dual functions: for instance BNDD was concerned on the one hand with domestic drug law enforcement activities and on the other hand with the curtailing of international narcotics trafficking. It would be to the latter area of responsibility that the National Security Agency delivered its intelligence. However, since the intelligence was being reported to some agencies which did have law enforcement responsibilities, there was growing concern that the intelligence could be used for purposes other than foreign intelligence. To minimize this risk, the material was delivered only to designated offices in those agencies and the material was marked and protected in a special way to limit the number of people involved and to segregate it from information of broader interest.

#### WATCH LIST ACTIVITIES AND TERMINATION THEREOF

In 1973, concern about the National Security Agency's role in these activities was increased, first, by concerns that it might not be possible to distinguish definitely between the purpose for the intelligence gathering which NSA understood was served by these requirements, and the missions and functions of the departments or agencies receiving the information, and second, that requirements from such agencies were growing. Finally, new broad discovery procedures in court cases were coming into use which might lead to disclosure of sensitive intelligence sources and methods.

The first action taken was the decision to terminate the activity in support of BNDD in the summer of 1973. This decision was made because of concern that it might not be possible to make a clear separation between the requests for information submitted by BNDD as it pertained to legitimate foreign intelligence requirements and the law enforcement responsibility of BNDD. CIA had determined in 1973 that it could not support these requests of BNDD because of statutory restrictions on CIA. The National Security Agency is not subject to the same sort of restrictions as CIA, but a review of the matter led to a decision that certain aspects of our support should be discontinued, in particular the watch list activity was stopped. NSA did not retain any of the BNDD watch lists or product. It was destroyed in the fall of 1973 since there was no purpose or requirement to retain it.

With regard to "watch lists" submitted by FBI, CIA and Secret Service, these matters were discussed with the National Security Agency Counsel and Counsel for the Department of Defense, and we stopped the distribution of information in the summer of 1973. In September 1973, I sent a letter to each agency head requesting him to recertify the requirement with respect to the appropriateness of the request including a review of that agency's legal authorities.

On 1 October 1973, Attorney General Richardson wrote me indicating that he was concerned with respect to the propriety of requests for information concerning U.S. citizens which NSA had received from the FBI and Secret Service. He wrote the following:

"Until I am able more carefully to assess the effect of *Keith* and other Supreme Court decisions concerning electronic surveillance upon your current practice of disseminating to the FBI and Secret Service information acquired by you through electronic devices pursuant to requests from the FBI and Secret Service, it is requested that you immediately curtail the further disseminations of such information to these agencies.

Of course, relevant information acquired by you in the routine pursuit of the collection of foreign intelligence information may continue to be furnished to appropriate Government agencies . . . ."

The overall result of these actions was that we stopped accepting "watch lists" containing names of U.S. citizens and no information is produced or disseminated to other agencies using these methods. Thus, the "watch list" activity which involved U.S. citizens ceased operationally in the summer of 1973, and was terminated officially in the fall of 1973. As to the future, the Attorney General's direction is that we may not accept any requirement based on the names of U.S. citizens unless he has personally approved such a requirement; and no such approval has been given. Additionally, directives now in effect in various agencies also preclude the resumption of such activity.

General ALLEN. Sir, with your permission, I may make some concluding remarks after the questions, if I may.

The CHAIRMAN. Very good. Thank you very much for your initial statement.

With respect to the legal questions that are raised by the various watch lists that you have described, I might say for the benefit of everyone concerned, that it is the committee's intention to call on the Attorney General in order that the questions regarding the possible illegality of these watch list operations, and also questions relating to the constitutional guarantees under the fourth amendment, can be taken up with the proper official of the Government—the Attorney General of the United States. We would hope to have Attorney General Levi here to discuss the legal and constitutional implications of your statement at a later date, perhaps next week. So I would hope that on that score, members would not press you too far since the proper witness, I think, is the Attorney General.

General ALLEN. Yes, sir.

The CHAIRMAN. Now, Mr. Schwarz will commence the questions.

Mr. SCHWARZ. Mr. Chairman, I would like to ask just two questions which lay a factual basis for the questioning of the Attorney General, and I hope that is not out-of-line in light of your comment. They are not designed to have him discuss law, but to lay a factual basis for a dialog next week.

The CHAIRMAN. Very well. We will listen to your questions and then pass on them.

Mr. SCHWARZ. Very well. General Allen, were any warrants obtained for any of the interceptions involving U.S. citizens which you have recounted in your statement?

General ALLEN. No.

Mr. SCHWARZ. And the second question: you have stated that NSA does not, in fact, intercept communications which are wholly domestic. That is, communications between two domestic terminals, and that its interceptions are limited to wholly foreign, or second terminals, one of which is in the United States and one of which is outside. With respect to wholly domestic communications, is there any statute that prohibits your interception thereof, or is it merely a matter of your internal executive branch directives?

General ALLEN. My understanding, Mr. Schwarz, is that—at least the NSC intelligence directive defines our activities as foreign communications, and we have adopted a definition for foreign communications consistent with the Communications Act of 1934. And therefore, I think that is the—

Mr. SCHWARZ. But you believe you are consistent with the statutes, but there is not any statute that prohibits your interception of domestic communication.

General ALLEN. I believe that is correct.

Mr. SCHWARZ. I have nothing further, Mr. Chairman.

The CHAIRMAN. Just so I may understand your last answer, General, so that the definition of foreign intelligence is essentially one that has been given you by an executive directive from the NSC, and is not based upon a statutory definition.

General ALLEN. Yes, sir.

The CHAIRMAN. Very well. We are going to change our procedures today to give the Senators at the end of the table who are usually the last to ask questions, and sometimes have to wait a good length of time, instead of moving from the chairman outward. This I must say, has the consent of our vice chairman, Senator Tower—so we will move to the ends of the table first, and that means our first Senator to question is Senator Hart.

Senator HART of Colorado. Thank you, Mr. Chairman.

General Allen, there are two broad areas that this committee is concerned about in terms of legislative recommendations. One is congressional oversight, and the other is the issue of command and control. And it is in these two areas that I would like to ask a couple of questions.

First of all, you went to some lengths in your statement to talk about the history of NSA's briefing of Congress and various congressional committees. In that history, was there any occasion when officials of the NSA briefed members of Congress about the watch list activities?

General ALLEN. Sir, I honestly don't know about that, prior to my coming on in the summer of 1973. And the reason for that is that the testimony is in executive session—and there are conversations, and I really don't know whether previous Directors discussed it with Congress or not.

I would say that I have no evidence that they did.

Senator HART of Colorado. That they did or did not?

General ALLEN. I would say that I have no evidence that previous Directors discussed the watch list matters with Congress prior to the summer of 1973 when I came on board. Since I went on board, there have been a number of occasions where this has been discussed with various elements of Congress which, to a certain degree, began early in 1974 with the investigations of the House Appropriations Committee investigating team.

Senator HART of Colorado. With what degree of specificity did you brief elements as you say, of Congress about the watch list activities? With the same degree of specificity that is contained in your statement today—the numbers of names and so forth?

General ALLEN. The investigation that I refer to by the Appropriations Committee investigative team did go into the matter in substantially more detail than we have described today. There were a number of pages in their report that we related to that.

I would suspect that other briefings probably were of less detail—well, no, I would say the briefing before Mr. Pike's committee was in more detail, discussed today, in closed session.

Senator HART of Colorado. For the purposes of our record today, did you conduct some historical review, whether, prior to your assumption of the Directorship, such briefings on watch list activities took place?

General ALLEN. Well, to the extent that we're able to conduct those activities, we have. And we have no evidence that they did take place.

Excuse me, I have just been pointed out an exception to that, and that is, Mr. Nedzi was briefed on the—at a previous time on the general subject of how these kinds of communications are handled. And I presume that he was given a fairly thorough insight into this.

Senator HART of Colorado. Do you know when that was?

General ALLEN. We will find that out, sir.<sup>1</sup>

Senator HART of Colorado. The same question applies to the other program which we have under consideration here today, and over which there is some dispute.

Could you tell us whether Congress, or any elements of Congress, were briefed on that program?

General ALLEN. I do not know. I do not know that they were.

Senator HART of Colorado. If you could find out and let us know, I think we would appreciate it.

The second broad area is the area of command and control: Who is in charge here? Who gives the orders? How high up are the officials who know what is going on? In this connection, it is my understanding that officials presently at NSA have testified, or given us information, that your predecessor, Admiral Gayler, and the former Deputy Director, Dr. Tordella, were completely aware of the watch list program, and their sworn testimony in the case of each or both of them is that they were not aware of this, or only became aware of it sometime after they assumed their positions.

Could you give us a definitive answer as to whether both Admiral Gayler or Dr. Tordella knew about the watch list activities?

General ALLEN. I am certain they did, sir. And I think the testimony you refer to must be misinterpreted in some way, because clearly, Admiral Gayler and Dr. Tordella knew, and have testified—I think, perhaps, sir, you may be referring to a question that did arise in our more complete closed discussions with the staff in which there was a question as to whether these analytic amplifications which NSA made to the lists—that is, where names were added by NSA people to enhance the selection process of the requirement already specified—whether those were approved by the proper command structure within NSA. And there has been a little bit of uncertainty about that.

It is fairly clear to me in my research that there was an appropriate Directorship, Deputy Director review of those procedures. It has been a little unclear as to whether each name was approved, and so on.

Senator HART of Colorado. In that connection, Admiral Gayler was asked, "Did people tell you the list included names of U.S. citizens or other entities?" and then came a rather long answer which includes

---

<sup>1</sup> In a Nov. 6, 1975, letter from David D. Lowman, Special Assistant to the Director, NSA, the select committee was informed that the date of the briefing referred to above was Jan. 10, 1975.

the following statement: "This particular subject didn't come to my attention until about the time this domestic problem was surfaced by the President."

The staff then asked, more specifically, when that was, and he said, "I became aware of that, I guess it was a year or so after I got there." So Admiral Gayler does not suggest that he was briefed on the existence of watch list activities until perhaps more than a year after he assumed the Directorship.

Do you know why that would be?

General ALLEN. No, sir, I don't. I was not aware of that aspect of his testimony. I do know, for example, of information that has been made available to the committee, that he was aware, and made fully aware, in 1971, early 1971 [exhibit 5].<sup>1</sup> Your time refers, actually, to before that.

Senator HART of Colorado. When did he assume the Directorship? In 1969?

General ALLEN. Yes; it must have been 1969. Yes, sir.

Senator HART of Colorado. So a period of time passed in which the Director of NSA apparently did not know that this activity was going on. We find that extraordinary.

You have stated that NSA officials or personnel were placing names on the list. There seems to be some dispute about that also. Admiral Gayler and Dr. Tordella both deny that they knew that NSA was putting names on the list, yet, I think the suggestion here is that this was knowledge that the Director and the Deputy Director didn't know about.

Is that the case?

General ALLEN. Well, we have clearly had a conflict in people's recollections in that period of time. It is the clear recollection—and there certainly are some internal memorandums that reflect—that the procedures by which amplifications are made to lists were explained to the Director and Deputy Director at the time, and that they were aware of them.

It apparently is also true that in the period of time when they gave testimony, they didn't recall that particular briefing.

Senator HART of Colorado. Well your testimony here this morning is a little confusing also. In your statement you say, we do not generate our own requirements for foreign intelligence, and yet the indication is that the staff or officials of NSA, do, or had in the past, added names out of the Office of Security, and so forth.

General ALLEN. I'm sorry, sir, that is another question. That does not actually relate to foreign intelligence. I believe it is not the subject of discussion today.

The question of adding names that relate to the amplifications in the foreign intelligence field was in no case a matter of adding anything new to the list. It was a matter of adding aliases, it was a matter of adding addresses in some cases where an organization had been specified, and it would assist picking up messages of that organization, the names of officials of the organization were added to enhance the selection process.

Senator HART of Colorado. But it is your testimony that out of the NSA itself there was no generation of new names or organizations?

---

<sup>1</sup> See p. 156.

**General ALLEN.** That is correct.<sup>1</sup>

Senator HART of Colorado. In connection with the role of the Intelligence Board, you indicate in your statement that the U.S. Intelligence Board reviewed these activities and was kept cognizant of them. We have testimony—statements before this committee by people involved in the Board's activities in the past, that the Board itself, in being apprised that watch list activities were going on was not aware of the fact that communications of U.S. citizens were being monitored.

Is that the case, or not?

General ALLEN. Well the difficulty that we have here, sir, as I understand it, is there is no record that the U.S. Intelligence Board in its sessions ever considered or had this information presented to them. The circumstances are that the requirements process of the U.S. Intelligence Board, which is directed toward substantive requirements, did include in it various subject statements—that is, that related to these particular subjects. And on occasion, included such subjects as in satisfying the watch list individuals provided by whatever agency it was. So those things are in the U.S. Intelligence Board guidelines. It could be only presumed that U.S. Intelligence Board, which consists of membership of the requesting organizations, knew that the lists they were directing to us to follow were lists which their agency was preparing and did contain some U.S. names.

Senator HART of Colorado. And therefore, it is your testimony, or is it not, that the intelligence board knew that so-called civil disturbance names were being included on this list?

General ALLEN. Well, the U.S. Intelligence Board certainly knew that, because my predecessor, General Carter, made it a very specific point to notify them immediately upon getting what he considered to be the first request in this area. And that was his purpose for doing that.

Senator HART of Colorado. Including the civil disturbance names?

General ALLEN. Well, yes, sir. His message is here in the record [exhibit 2]<sup>2</sup>, but it states that he is being asked to respond to this requirement and to seek intelligence regarding foreign influence on certain organizations.

Senator HART of Colorado. One final question, General.

In connection with the Huston plan, one recommendation of that group was that communications intelligence capabilities should be broadened and that the President was requested to authorize broadening of those capabilities.

To your knowledge, did President Nixon know about the extent of this watch list?

General ALLEN. To my personal knowledge?

Senator HART of Colorado. Well, to your knowledge as Director.

General ALLEN. No. I have no such knowledge one way or another as to President Nixon's personal knowledge.

---

<sup>1</sup> After reviewing a transcript of this testimony, NSA advised the committee that 50 to 75 names were added in its "amplification" of watch lists, and that this "was usually done either by adding the name of an executive officer of an organization, or by adding the organization name associated with a person who was placed on the watch list by another agency." (Letter from David D. Lowman, Special Assistant to the Director, NSA, to the select committee, Nov. 6, 1975.)

<sup>2</sup> See p. 147.

Senator HART of Colorado. So you, or perhaps Mr. Buffham, can't account for the fact that the President was being asked to broaden a capability that he did not know existed in the first place?

General ALLEN. Well, you asked me what I thought President Nixon knew.

Senator HART of Colorado. Yes.

General ALLEN. And I say I really don't know. There is some evidence as to what Mr. Huston thought because we have the various things which he wrote, and the documents that he prepared. Mr. Huston apparently believed that this activity which he knew of, and which he had seen the output of, was being conducted in a very restrictive and minimal manner—which was true—and that it would be of value to those problems which the President had on his mind if it were expanded. And he also recognized that the NSA would not respond to that kind of a request for expansion or broadening of this activity without very clear and specific Presidential direction to do so. So it is my understanding that Mr. Huston was making such a recommendation, and of course it did not come to pass.

Senator HART of Colorado. That is all, Mr. Chairman.

Thank you.

The CHAIRMAN. Thank you, Senator Hart.

Senator SCHWEIKER?

Senator SCHWEIKER. Thank you, Mr. Chairman.

General Allen, who were the two Attorneys General and the Secretary of Defense who approved this activity?

General ALLEN. Our statement said they reviewed the activity.

Senator SCHWEIKER. Reviewed it?

General ALLEN. Yes, sir. We have documentation available in looking back at our records of this, that Admiral Gayler reviewed this activity in detail with Mr. Laird, Mr. Kleindienst, and Mr. Mitchell, on a couple of occasions, one very clear one relating to Mr. Laird and Mr. Mitchell. Approval is an awkward—it is not fair to those people in the sense that the memo for record shows that he discussed it with them in some detail, that there was agreement as to the procedures that were to be followed, and that he then submitted a memorandum back to them saying this is what we discussed and this is the procedure we followed.

Senator SCHWEIKER. That is Admiral Gayler reviewed it with him—with them, I should say?

General ALLEN. Yes, sir.

Senator SCHWEIKER. And then, just a moment ago, we heard there was some discrepancy as to whether Admiral Gayler knew about the watch list himself.

General ALLEN. Well sir, that was at the time—apparently Admiral Gayler's recollection had to do with a year or so afterward. I believe, as we look back at the records, it is probably true that that was not quite so long as a year.

Senator SCHWEIKER. General Allen, in the course of intercepting international communications, does the NSA accidentally or incidentally intercept communications between two American citizens if one of them happens to be abroad?

General ALLEN. Yes, sir.

Senator SCHWEIKER. And what procedures, and what do you do after you intercept a message between two American citizens, either in terms of what you feel the law is or what your directives are?

General ALLEN. The directives are that we do not do anything to those communications, and we reject it as early—reject such communications as early in the process as it is possible for us to do. For example, if by tuning the receiver, it is possible to reject them, that is what one does. It turns out to be somewhat later in the process, one does it then. But the rules are clear, and that is that one rejects those messages as quickly in the selection process and as automatically as it is physically possible to do.

Senator SCHWEIKER. Is there any law that you feel prohibits you from intercepting messages between American citizens if one is at a foreign terminal and the other is at a domestic terminal, or do you feel there is no law that covers this situation?

General ALLEN. No, I do not believe there is a law that specifically does that. The judgment with regard to that is an interpretation.

Senator SCHWEIKER. General Allen, in a few words, what was Project MINARET? Would you just describe, just briefly, what the objectives of Project MINARET was?

General ALLEN. Well, sir, that was the project we have been talking about. That was a code word used for it during part of the time we described.

Senator SCHWEIKER. Relating to the individuals, organizations involved in civil disturbances, antiwar movements, demonstrations, and things such as that; is that correct?

General ALLEN. Yes, sir. MINARET is a term that began in 1969, and as we described somewhat formalized the process by which these messages were handled, which had begun apparently about 1967 [exhibit 3].<sup>1</sup>

Senator SCHWEIKER. Now, in the initial communication on MINARET, is it true that one of the equally important aspects of MINARET was not to disclose that NSA was doing this?

General ALLEN. That appears in the documentation regarding it. Yes, sir.

Senator SCHWEIKER. And what was the reason for not disclosing to the other intelligence agencies—because this information only went to other intelligence agencies—what was the reason for not disclosing to the other intelligence agencies, who were the consumers, that NSA was doing this?

General ALLEN. It is hard for me to really answer it, because I am not exactly sure as to what was the feeling of the people at the time. My understanding is that the concern was that the people at NSA felt it was terribly important that the activity be solely related to foreign intelligence, and that by delivering these kinds of messages to an agency which also had a law enforcement function, there was a danger that the material would end up being used for a purpose which would not be appropriate. Therefore, for that reason there were a set of procedures adopted which made the material be handled in a distinctive and separate way to where it went to only specified individuals, only hand-carried, clearly marked "For Background Use Only;" also de-

---

<sup>1</sup> See p. 149.

void of the kind of designators that are placed on the kind of intelligence information which NSA produces for a broader range of users.

Senator SCHWEIKER. Might there have been some concern that this was a questionable legal area and that therefore dissemination of who was doing it and how they were doing it might also have been injurious to the Agency?

General ALLEN. It is possible. I think that of course the concern was that if the material was—the basic concern is, I imagine it was in people's minds at that time, was that if the material were used for some purpose associated with prosecutive or evidentiary basis, that the sources and methods which were used to obtain that intelligence would then be vulnerable to disclosure or demands by courts to see it; so there was a very great concern to insure that this material was handled in such a way as to minimize the possibility that it would be used in that fashion.

Senator SCHWEIKER. Would it be possible—granted this is not your policy, and that you state you have not done this—would it be possible to use this information and apparatus that you have to monitor domestic conversations within the United States if some person with mal-intent desired to do it? Not that you have done it, not that you intend to do, not that you don't have a prohibition about it; I am just asking you about capacity or capability.

General ALLEN. I don't think I really know how to answer the question. I suppose that such a thing is technically possible. It is clearly in violation of directives procedures which are established throughout the entire structure and which are monitored with great care.

Senator SCHWEIKER. And it has not been done by your agency, is that correct?

General ALLEN. Yes, sir.

Senator SCHWEIKER. The names that were put on the watch list could have been sent in by any one of almost, I guess, a dozen security agencies or intelligence agencies. Did you have any criteria as to whether you accepted their names or not? In other words, suppose the FBI put names on a list; did you reject any of their names, or did you just accept that as the input and the recommendation or the suggestion from the FBI, for example?

General ALLEN. It is my understanding, in going back and discussing how that process worked at that time, that there were, in at least two cases, discussions about substantial increases to names for a couple of different problems. These problems looked to the people at NSA as though they were in the law enforcement area, and therefore these agencies were told not to submit those kinds of names, and they were not so submitted. So, there was that kind of a review made, at least in some cases.

In general it is true that the agencies did submit names and NSA accepted them based on the assurance of senior officials at those agencies that that was an appropriate thing to do.

Senator SCHWEIKER. So, it is NSA's basic position that the responsibility as to determining what criteria was used for putting names on the list, with the exceptions you have noted in terms of specifics, was basically the responsibility of the originating agencies, is that correct?

General ALLEN. Yes, sir. You will note in the record that when I arrived at NSA, one of the first things that I did was to contact each

of the agency heads and request them to reexamine exactly that point, and to reassure me that they had reviewed these names on the list and that their requests for information were appropriate within their statutory and executive authorities. That, of course, ended up with having the effect of terminating the program. But the view that we had was that that responsibility was one held by the requesting agency.

Senator SCHWEIKER. Do you think that the responsibility should rest with each agency? I am thinking of prospective legislation. Where do you think that responsibility should lie as to who makes demands on your agency at this point for the future? Shall we forget the past?

General ALLEN. Well, for the future, we certainly have directives now which prohibit this kind of activity in the future, and those are internal NSA directives which I have issued. There are also, I understand, similar directives at the requesting agencies. I believe that it has to be a responsibility of both, and I think the question of oversight was in the executive branch is one that is appropriate for the executive.

Senator SCHWEIKER. Yes. And yet, Mr. Huston wrote a memo that we referred to a moment ago, where the memo indicated, at least as far as the memo was concerned, he wasn't even aware that the kind of activity we are talking about was going on. This was a memo to Haldeman, to the whole White House structure, and unless somebody was misleading people in terms of writing a false memo, or badly informed, the memo went out implying that none of this activity really was being conducted now.

Is that not correct?

General ALLEN. No, sir, that is not correct.

Senator SCHWEIKER. The Huston memo didn't say that you needed more authority to do what you were doing?

General ALLEN. The Huston memo, according to my recollection, sir, said that the NSA was providing some intelligence pertinent to this problem at the present time in accordance with very restrictive and in a minimal way, and that in order to do more of it, presumably in accordance with the President's desires, they would have to receive additional instructions in order to do that.

Senator SCHWEIKER. Yet, the watch list was going on in full blast at the time with any agency having a right to put in any name that they wanted. I have trouble reconciling that.

General ALLEN. Well, Number one, sir, I am not sure what you mean by "full blast." The program I described was in process. Agencies were, I trust, constrained in their placing names on it, and NSA at least exercised some constraints in their accepting of names. There was a great deal of constraint in the manner in which the information was handled. There were also no activities undertaken by NSA, with the one exception we noted, to obtain these communications, only to select them. And, it was to these issues, I think, that Mr. Huston was probably referring when he said he thought there should be an expansion.

Senator SCHWEIKER. One final question, General.

You testified that in 1973, the CIA decided to discontinue certain activities because those activities might be in violation of the CIA's statutory charter. Now, NSA has no such charter, and yet, I think obviously you, too, are concerned about the activities of the past.

Shouldn't we have a charter for NSA, and shouldn't we write into law some things that won't be misconstrued or misunderstood or might be abused in the future? Shouldn't NSA have a charter like the CIA does?

General ALLEN. Well, sir, I really must leave that judgment up to the Congress. It is certainly clear now that the directives relating to foreign intelligence, and that the interpretations of foreign communications as they are appropriate at this time, are both clear in executive directives, and are enforced.

Senator SCHWEIKER. Thank you, Mr. Chairman.

The CHAIRMAN. Thank you very much, Senator Schweiker.

Senator Morgan is next.

Senator MORGAN. General Allen, I noticed in your testimony that you said between the years 1967 and 1973 you had at most about 450 names on the watch list for the purpose of watching for narcotics. Is that correct?

General ALLEN. Yes, sir, I believe so.

Senator MORGAN. And about 1,200 other names altogether.

General ALLEN. Yes, sir.

Senator MORGAN. So during that period of time of about 6 years you had about 1,650 names on the watch list.

General ALLEN. Yes, sir.

Senator MORGAN. And I believe you said—

General ALLEN. U.S. names, sir.

Senator MORGAN. U.S. names, that is right. And that the most that you had at any one time was about 800 names.

General ALLEN. Yes, sir.

Senator MORGAN. Now all of these names, or U.S. names, were names that had been involved in communications between a foreign station and either this country or some other foreign station.

General ALLEN. Well, the reports which were generated as a result of those names fit that description, yes, sir.

Senator MORGAN. That is right. And you were watching, of course—you put those names on, you testified, for many purposes; one, in an effort to stem the narcotics traffic. Is that one of the reasons?

General ALLEN. Yes, sir.

Senator MORGAN. And I believe you testified earlier that some large shipments of narcotics were identified through this watch list and were prevented from coming into this country.

General ALLEN. That is my understanding, yes, sir.

Senator MORGAN. Well, that was your testimony and your best information, was it not?

General ALLEN. Yes, sir.

Senator MORGAN. You testified also that on one occasion an assassination attempt on a prominent U.S. figure abroad was identified and prevented by the use of this watch list. Is that correct?

General ALLEN. Sir, I would have to set the record straight. We did identify that in an earlier version. In reviewing that particular item, there is some question in our mind as to whether the actual watch list procedures that we described here were the reason for selecting out the message that made that revelation. So, in an attempt to be completely fair, I would like to not say that was a result of the watch list.

Senator MORGAN. It did come from a message though that you intercepted.

General ALLEN. Yes, sir.

Senator MORGAN. You gave us another example as a value of this service, a notification to the FBI of a major foreign terrorist act that was planned in a large city in this country, which action was prevented because of information you received?

General ALLEN. Yes, sir.

Senator MORGAN. Is this the sort of information that you are looking for and watching for?

General ALLEN. Yes, sir.

Senator MORGAN. In all that period of time, in all of those 6 years then, is it fair to say you had about 1,650 American names out of about 200 million Americans?

General ALLEN. Yes, sir.

Senator MORGAN. All right, sir. Now, have you made all of that information available to the members of this committee or to the staff of this committee in executive session before?

General ALLEN. Yes, sir.

Senator MORGAN. Now, there is another project that has been alluded to but has not been named here today. Have you also testified to the members of this committee and/or to the staff all the information relevant to that project?

General ALLEN. Yes, sir.

Senator MORGAN. Have you been willing at all times to disclose any and all information about the NSA to the members of this committee in executive session?

General ALLEN. Yes, sir.

Senator MORGAN. And are you still now ready—are you now ready and willing to disclose that or any other information?

General ALLEN. In closed session? Yes, sir.

Senator MORGAN. In closed session, to this committee of the United States Senate.

General ALLEN. Yes, sir.

Senator MORGAN. Now you testified also about the law with regard to this disclosure of information. If you would bear with me just a minute—I believe you testified that:

The Congress of the United States in 1933, both the House and the Senate, enacted a law encoded in 18 U.S. Code 952, which prohibits the divulging of the contents of decoded foreign diplomatic messages or information about them.

And you also said that:

Again in 1950, the Congress, both the House and the Senate, enacted another law, encoded in 18 U.S.C. 798, which prohibits the unauthorized disclosure, prejudicial use, or publication of classified information of the government concerning communication intelligence activities, cryptologic activities, or the results thereof.

Is it your opinion that that is still the law?

General ALLEN. Yes, sir.

Senator MORGAN. Is it your opinion that the information with regard to the other project, if disclosed publicly, would be detrimental or could be detrimental to the national security of the United States?

General ALLEN. Yes, sir.

Senator MORGAN. To your knowledge, is it still not the position of the President of the United States that that information should not be disclosed publicly?

General ALLEN. That is my understanding, sir.

Senator MORGAN. And the Attorney General of the United States has so communicated that to this committee. But you are still willing—in the first place, you have communicated that information, all that you have been asked for, to this committee and you are now willing to communicate any other information within your command to this committee in executive session.

General ALLEN. Yes, sir.

Senator MORGAN. All right. Thank you, sir. Thank you, Mr. Chairman.

The CHAIRMAN. Thank you, Senator Morgan.

Senator Mathias?

Senator MATHIAS. Thank you, Mr. Chairman.

General, on the last page of your statement, you say that:

Thus, the watch list activity, which involved U.S. citizens, ceased operationally in the summer of 1973 and was terminated officially in the fall of 1973.

I think that is perhaps the most important sentence in your statement. And I want you to tell us if that is now the status.

General ALLEN. Yes, sir, it is.

Senator MATHIAS. And this was done on the advice of Attorney General Richardson, but in fact, by the agency itself. Is that correct?

General ALLEN. Yes, sir. I terminated the—well, the distribution of materials was terminated in the summer. I requested each of the agencies to review it and it was shortly after that that the Attorney General also then wrote to me and said he was questioning the requests from FBI and the Secret Service.

Senator MATHIAS. Well, this is the kind of judgment and restraint that I wish more of the agencies of the Government had exercised throughout the years. I think, General, you are to be congratulated for the action that you took. I think it is a very important addition to the administrative history of the Federal Government. I think it is an example that I wish others would follow.

I have no further questions.

Senator GOLDWATER. He is Air Force, that does not surprise me.

Senator MATHIAS. Do you want that on the record?

General ALLEN. Yes, sir.

The CHAIRMAN. Senator Mondale?

Senator MONDALE. Thank you, Mr. Chairman.

General Allen, I would like to say for the record that I think that the work of the NSA and the performance of your staff and yourself before the committee is perhaps the most impressive presentation that we have had. And I consider your Agency and your work to be possibly the most single important source of intelligence for this Nation. Indeed, so much so that I am not convinced that we fully perceived the revolution that has occurred in recent years in intelligence gathering as a result of technological breakthroughs, and it is your agency which basically deals with that area. But it is that most impressive capacity which works so often for the purposes of defending this country and informing it that also scares me in terms of its possible abuse. That is why I am interested in knowing what limitations exist, in

your opinion, upon its use that could be described as an abuse of the legal rights of American citizens. As I understand your testimony, you limit yourself to the interception of communications between—either to or from—a foreign terminal and one in the United States. You do not intercept messages to and from persons within the United States.

General ALLEN. That is correct, sir.

Senator MONDALE. But I also understand that this is a matter of policy and not of law, that the basis for this limitation is a judgment on the part of our Government that that ought to be as far as you go. There is not, in your judgment, or in the judgment of the Agency, a restriction that would limit you precisely to those policy guidelines that you now have.

General ALLEN. Well, I believe that is correct, sir, as far as the precise restriction is concerned. But there is no misunderstanding with regard to the Executive directives that exist, the restriction is to foreign intelligence purposes and foreign communications which are defined in some way.

Senator MONDALE. Given another day and another President, another perceived risk and someone breathing hot down the neck of the military leader then in charge of the NSA; demanding a review based on another watch list, another wide sweep to determine whether some of the domestic dissent is really foreign based, my concern is whether that pressure could be resisted on the basis of the law or not.

General ALLEN. Well, it is very hard for me, of course, to project into a future unknown situation. And there are certainly risks that seem to have occurred in the past. I can certainly assure you that at the present time, under any combination of the present players, as I understand the rules and the players themselves, there is no possibility of that.

Senator MONDALE. I will accept that. But what we have to deal with is whether this incredibly powerful and impressive institution that you head could be used by President "A" in the future to spy upon the American people, to chill and interrupt political dissent. And it is my impression that the present condition of the law makes that entirely possible. And therefore we need to, in my opinion, very carefully define the law, spell it out so that it is clear what your authority is and it is also clear what your authority is not.

Do you object to that?

General ALLEN. No, sir.

Senator MONDALE. I am very heartened by that answer. In the old days of the watch list, as I understand our earlier testimony, when a name was presented to you from the FBI, from the CIA, or from other sources, your agency really could not determine whether the purpose of including that name was for a legal objective or for an illegal purpose. In a sense, your role was largely ministerial. The names were received. They were placed on the watch list. You intercepted information and sent it to the consumer agency. But why they really asked for it, other than the very generalized description they would often give you, or how the information was used, was largely unknown to the NSA. Is that correct?

General ALLEN. Well, it is certainly to some degree correct, sir. The points that you have made were recognized at the time and there were

steps taken to try to protect against the dangers that you point out. For example, there was, as a matter of practice, a description of the foreign intelligence requirement to which names were requested.

Senator MONDALE. Yes, they would say this would be for drugs or this is for personal security of the President, or this is for the purpose of determining whether there is foreign influence in terms of the antiwar movement, and so on. But there was no way that you really knew in most cases, what may have been behind a request or how that information was being used. Was there?

General ALLEN. Yes, sir. In a strict sense that is certainly correct.

Senator MONDALE. Thus similarly, the IRS is in the same position that if some agency like the FBI in its COINTEL Program is pursuing an illegal objective, you may be tasked to intercept messages in order to procure information for an illegal purpose. That too, then, ought to be defined very carefully to protect your agency from abuse. Would you agree with that?

General ALLEN. Yes, sir.

Senator MONDALE. I find that answer heartening.

During the watch list days, you were oppressed heavily, along with the other agencies, to find evidence of foreign involvement, direction, or control of the antiwar movement. Would you say that you found much evidence of such foreign control and direction?

General ALLEN. Sir, my understanding of that is not complete. From a review of results of those messages which we did provide other agencies, they essentially did deal with foreign influences and foreign support to certain domestic activities. And so, in that sense, I would say that the results of the NSA activity did show foreign influence. It is also my understanding that when that information was put in perspective by particularly the CIA, I believe, that their conclusion was that the degree of foreign control was very small.

Senator MONDALE. The first part of your answer surprised me a little bit because almost uniformly we have heard evidence from the various other agencies that they found little or no foreign direction, even though they were being pressed so hard to find it by the—

General ALLEN. Well sir, you must bear in mind that we were only dealing with messages that related to a foreign contact or a foreign interaction for the person involved. So all we saw was that. And so our perspective on it is clearly biased. What we saw was foreign involvement and foreign support. I don't want to use the word control because I do not know how to assess that. But my understanding is that the agencies evaluating it concluded as you said.

Senator MONDALE. One of my concerns, and I think this has come up with the other agencies—the Postal Department, the IRS and so on—is that when you are tasked to review something as vague as foreign involvement or direction, it becomes so vague that it is very hard to restrain the review at all. And we have one example that it is agreed that we could raise today. A leading U.S. antiwar activist—and we know him to be a moderate, peaceful person, as a matter of fact, someone who quit the antiwar movement even though he was desperately against the war, because he so much opposed some of the militancy and violent rhetoric—sent a message to a popular singer in a foreign country asking for contributions to a peace concert—and also his participation. The message noted the planned participation

in this concert of some of the most popular musicians and groups in the United States at that time and asked the recipient "either to participate directly in providing the entertainment, or support the concert financially." Now, we have agreed not to use the names. I do not know why we have agreed not to use the names, but we have.

The CHAIRMAN. I might say there, Senator, the reason being that we have not first cleared it with these individuals and there is a matter of their own privacy that we have to take into account.

Senator MONDALE. All right, fine. But in any event, when you are picking up stuff like this from peaceful people who just are opposed to a war which now most Americans feel was unwise, do you not think that it raises very serious questions about how you contain snooping and spying on American citizens—particularly when your agency is required to pursue an objective which virtually defies definition and so easily can spill over in a way to undermine and discourage political criticism and dissent in this country?

General ALLEN. I am afraid, sir, I have to dodge the basic philosophic nature of your question because the facts are, that as a technical collection agency, NSA was asked a far more simple question, which is a little hard for me to go back and construct all the emotion at the time. It is certainly not the same as today. But that question was that the Defense Intelligence Agency, in this particular case, asked for information on the funding of certain U.S. peace and anti-Vietnam war groups. And this message was from such an organization or person to an overseas location where foreign funding and support was requested. It's certainly true that in this time in history one would certainly have a substantially different view of that than at the time.

Senator MONDALE. But it shows how very difficult it is to define the outer parameters of a search like that, does it not? I mean, if we could use the names today, I think people would be surprised at governmental concern or the feeling that Government had the right to snoop in such messages, would they not?

General ALLEN. Well, I only can say I don't know how to answer your question. The requirement to us, the request for information was very specific and very constrained and addressed to a very narrow point. The broader aspects of your question, I think I am not really qualified to answer.

Senator MONDALE. I think that is why we have to define your requirements to include some very precise limits on the interruption of citizens' rights, because as I see it now, at least as the agency has defined its restrictions in the past, you are largely unrestricted. It has been the interpretation of your agency that you can roam very far indeed.

Thank you very much, Mr. Chairman.

The CHAIRMAN. Thank you Senator Mondale.

Senator Goldwater.

Senator GOLDWATER. First, I want to be on the record as opposed to public hearings on this matter.

General, as I remember correctly, when you were before our committee, you stated that the law did not allow you to testify on any aspect of the NSA. Is that correct?

General ALLEN. That is what I believe to be the case, yes, sir.

**Senator GOLDWATER.** Then, theoretically, you are violating the law in being here.

**General ALLEN.** It would seem so, yes, sir.

**Senator GOLDWATER.** Well I wanted to ask that question to get two rules that bear on this committee that maybe some of our members have forgotten about.

In the Senate Rule 36 paragraph 5 it says:

Whenever, by the request of the Senate or any Committee thereof any documents or papers shall be communicated to the Senate by the President or the head of any Department relating to any matter pending in the Senate, the proceedings in regard to which are secret or confidential, under the rules, said documents and papers shall be considered as confidential and shall not be disclosed without leave of the Senate.

I wanted to make that a part of the record in the event that any classified information might be offered by members of this committee under the assumption that we have the power to downgrade or down-classify classified information.

Then, we in our own rules, under Senate Resolution 21 "a select committee is required to protect classified information."

Section 7 reads as follows:

The Select Committee shall institute and carry out such rules and procedures as it may deem necessary to prevent . . . (2) the disclosure, outside of the Select Committee, of any information which would adversely affect the intelligence activities of the Central Intelligence Agency in foreign countries or the intelligence activities in foreign countries of any other department or agency of the Federal government.

So you are probably, in your opinion, operating outside the law. I just wanted to set the stage so that this committee would not try to operate outside the rules of the Senate and the rules of its own committee.

I have no questions.

**The CHAIRMAN.** Thank you Senator Goldwater.

I think at the appropriate time I will reply to the suggestion that the committee is operating outside of the rules of the Senate or outside of the law. I do not believe that to be a correct statement of the position of this committee. But I will not interrupt the line of questioning at this time, because I think Senators would like to have a chance to complete the questioning of the witness.

**Senator GOLDWATER.** Mr. Chairman, I did not charge that we had operated outside the rules. I said we may.

**The CHAIRMAN.** Very well, we will discuss that at greater detail unless the Senator would like to discuss it now. I thought we would go through the line of questioning first.

**Senator GOLDWATER.** I just want to protect you and all of us.

**The CHAIRMAN.** All right, fine. Thank you Senator Goldwater. I really appreciate that.

**Senator TOWER.** I must say, Mr. Chairman, I am very touched by Senator Goldwater's concern for your safety.

**The CHAIRMAN.** I am too, Senator. Let us see, who is next here? Senator Baker.

**Senator BAKER.** Mr. Chairman, thank you very much.

General, I notice in your statement in speaking of the utilization of the watch list and your efforts in that respect over the years. This sentence: "Examples of the value of this effort including the notifica-

tion to the FBI of a major foreign terrorist act planned in a large city which permitted action to prevent completion of the act and thus avoid a large loss of life." Are you at liberty to elaborate on that at this point?

General ALLEN. I really am not, sir.

Senator BAKER. And the balance of the statement is equally provocative to me. It says: "An assassination attempt on a prominent U.S. figure abroad was identified and prevented." Can you give us any further information on that? I am not urging you to go beyond the confines of those things you are permitted to testify to at this point.

General ALLEN. Sir, we will certainly provide that in executive session to you and go into some detail.

Senator BAKER. On both those points in executive session?

General ALLEN. Yes.

Senator BAKER. Then I will not, General, insist on it at this time except to ask you whether or not I am to assume by your statement that both of these activities, which I will hear more about in executive session later, were in fact prevented as a result of your activities in conjunction with the watch list.

General ALLEN. No, sir. Well, Senator Morgan asked the question and you have an earlier draft of the statement, the one with regard to the assassination attempt, on more careful review, we really could not support that it was a watch list entry that caused us to select the message that revealed that particular act. So that was an error on my part to have included that. The situation is correct in the interception of the message and all of that is correct. But it is unfair to say that we selected because of the watch list.

Senator BAKER. But both of them were involved with your watch list activities.

General ALLEN. Yes, sir.

Senator BAKER. Well I will look forward to your further statement on that a little later.

On the general watch list operations, General, did you ever receive the written approval of any Attorney General of the United States about these activities?

General ALLEN. Not to my knowledge, no, sir.

Senator BAKER. Was any ever sought that you know of?

General ALLEN. No, sir. The briefings which a predecessor of mine gave had some of those characteristics and the record shows that they were briefed in some detail and had some agreement on the procedures to follow. But it is probably unfair to the Attorneys General involved to say that it was a specific written approval.

Senator BAKER. Do you know of particular circumstances where a President or an Attorney General or any Cabinet member for that matter may have suggested names to be included on the watch list?

General ALLEN. No, sir, I do not.

Senator BAKER. Were any names ever suggested to the NSA that were rejected for inclusion on the watch list?

General ALLEN. My understanding, sir, as we have looked back at the history of that is that there were substantial numbers of names which were suggested, a large number from the FBI and from another agency as well which were rejected in the sense that a discussion took place as to the appropriateness of these names. The NSA people pointed

out to them that it was too close to law enforcement and that therefore they should not be included. And, therefore, they were rejected.

But that is not documented in the sense of it was turned down before it got to the Director of the FBI and he did not in fact submit the name.

Senator BAKER. That is a fairly general statement. But let me tell you the impression that I draw from it. You are saying that in these particular cases that the NSA said these names and the purposes for which you would include these names are not close enough to intelligence gathering, which is our bag, and are probably only justified as law enforcement, which is your bag, and therefore we are not going to include them.

Is that the essence of what you have said?

General ALLEN. Yes, sir.

Senator BAKER. Who made that determination? Did you make that determination?

General ALLEN. No, sir. It was made at a lower level within the agency, so the request never came. I am reminded it was actually not the FBI but the Department of Justice.

Senator BAKER. I see. All right.

General ALLEN. And it was turned down before it got to the Attorney General.

Senator BAKER. Thank you very much, Mr. Chairman.

The CHAIRMAN. Thank you, Senator Baker.

Senator BAKER. Before we go on, General I do want to be briefed on the other two points, Mr. Chairman, either in executive session or if the General would agree to fill me in on the details at a later time, I would be grateful for that.

The CHAIRMAN. Very well.

Senator Tower.

Senator Tower. General, you are familiar of course with the efforts that have been made by the committee, by representatives of the administration and your agency to be circumspect in this public inquiry. Now, taking into account that effort and the good faith of all concerned, is there, in your opinion, a substantial risk still that these open hearings may impact adversely on the mission of your agency?

General ALLEN. Yes, sir.

Senator Tower. Thank you, General.

The CHAIRMAN. General, your answer to the last question reflects the position of the administration, does it not, which is opposed to any public hearings on all matters past or present relating to the NSA.

General ALLEN. That was terribly broad, sir.

The CHAIRMAN. Well it seemed to me that the administration took a terribly broad position.

General ALLEN. I believe it is probably fair to say on all matters that relate to the intelligence operations of the NSA.

The CHAIRMAN. And it is also clear that although the administration opposed these hearings this morning on the watch list question, they did declassify the documents at the committee's insistence and did authorize you to appear as a witness this morning to respond to the committee's questions.

General ALLEN. That is correct, sir.

The CHAIRMAN. I have listened with great interest to your testimony, General, and to the answers. And it seems to me that the real area of concern for this committee has nothing to do with the fact that on occasion, your operation, watch list operation related to a perfectly good and important matter. I do not think that anybody here would quarrel about the fact that information affecting the protection of the President is a very important matter and if you have a capacity to help in that regard, I do not suppose any member of this committee would want to argue that that is irrelevant or unimportant.

The same thing can be said about narcotics. We are all concerned about narcotics. So our inquiry here has not as its purpose criticizing given objectives that you sought to serve, of the kind that you described. But, rather the lack of adequate legal basis for some of this activity and what that leads to. For example, you yourself testified that in connection with some information that you obtained on narcotics and turned over to law enforcement agencies of the Government, prosecutions could not be initiated because it was not possible to introduce that evidence into court. It was not lawful and under the rules of the court and laws of the land it could not be used. So prosecutions could not be initiated. Is that not correct?

General ALLEN. Well, I do not know sir. The reason that that concern was felt at the time was because the information could not be used in court because to do so would reveal intelligence sources and methods.

The CHAIRMAN. Well, for whatever reason we will question the Attorney General on the legality of the use of that information. But for one reason or another, it could not be used in actual prosecutions.

Now, Senator Mondale, it seemed to me, touched upon the root cause of our concern. Here we have an agency, the NSA, that is not based upon a statute, like the CIA, which undertakes to define its basic authority. And your testimony makes clear that whatever foreign intelligence may mean, it is being defined, from time to time by the executive. Is that not correct?

General ALLEN. Yes, sir.

The CHAIRMAN. Now, ordinarily, the executive does not decide such basic matters. Ordinarily, as in the case of the CIA, an agency of this importance finds its fundamental power derived from legislation. Suppose for example we had a President, we cannot be so certain what kinds of things may happen in this country, suppose we had a President one day who would say to you: "I have determined with my advisers, who are my appointees, that foreign intelligence is seamless and it is quite impossible to differentiate between domestic and foreign intelligence because we need to know it all, and some of it we can gather from domestic sources. And so, in the overriding interest of obtaining the maximum amount of foreign intelligence you are instructed to intercept messages between Americans that are purely domestic and various agencies of the Government will furnish you with lists of people whose messages you are to intercept—all without warrant, all without any judicial process, all without any sanction in the law."

Now, under those circumstances, is there anything in the present law that would permit you to say we cannot do this, Mr. President, and we refuse to do it because it is illegal?

General ALLEN. Yes, sir.

The CHAIRMAN. What provision is there in the law?

General ALLEN. It is my understanding that the interpretations which deal with the right to privacy of unreasonable search and seizure of the fourth amendment.

The CHAIRMAN. Well all of those questions—

General ALLEN. Those domestic intercepts which cannot be conducted under the President's constitutional authority for foreign intelligence, then we are not authorized by law or constitutional authority and they are clearly prohibited.

The CHAIRMAN. But those very questions were raised with respect to some of the watch list activities. In other words, do you not think that it would be in the interest of all of us if we had some statutory law like most all other agencies have that defines the basic mission and defines as a matter of law foreign intelligence and contains whatever other guidelines may be necessary to be sure that this tremendous capability you possess is outward looking and is confined to legitimate intelligence concerns of the country.

General ALLEN. Clearly, sir, neither I nor the agency I represent has objection to laws which are needed by this country. And we look to the Congress to make those decisions. On the other hand, I certainly do not want to leave the impression, sir, that there are these broad ranges of evil activities which would be done which in themselves—in my understanding of the status of the law and the executive branch directives—are clearly prohibited.

The CHAIRMAN. The executive branch directives which are largely determinative of the scope of your action at any given time are subject to change within the executive branch. The point I make is that there is a legislative responsibility here. And since it normally obtains with respect to the work of all other Federal agencies, it would seem to me advisable that it should also obtain with respect to the NSA.

I have no further questions of you General.

Are there any other further questions on the part of the members of the committee?

Yes, Senator Mondale.

Senator MONDALE. May I ask, is it Mr. Buffham?

General ALLEN. Yes, that is correct.

Senator MONDALE. If he is not sworn in, he doesn't have to be. I just want to ask, you were I understand, representing the NSA, or at least representing General Gayler, in the preparation of the Huston plan, is that correct?

Mr. BUFFHAM. Yes, sir.

Senator MONDALE. Can you help explain to us the mystery of why NSA appeared to be requesting authority from the President to do what it was already doing? What, in addition, was expected if the President signed off? What did you want to be able to do that was not then thought to be within the authority of the NSA?

Mr. BUFFHAM. Well, the activities which were ongoing at that time were very, very carefully controlled and very, very restrictive and very, very minimal.

The procedures which Senator Schweiker described under MINARET were drawn up to insure the most careful handling of this very, very restricted, very, very minimal effort. It appeared when this—when we were asked to cooperate by the President in providing more information that would be helpful in the domestic area, it ap-

peared to us that we were going to be requested to do far more than we had done before and it appeared to us that this might actually involve doing some collection, which we had never done before, doing some collection for this purpose. And we did not feel that we could engage in such activity unless there was approval at the very highest levels. So that was the reason that there was a reservation on NSA's part, and the feeling that any increase in these activities must have Presidential approval.

Senator MONDALE. So it was your judgment at that time that you were being asked, or were about to be asked, to do something that went substantially beyond—

Mr. BUFFHAM. That we could do, but we weren't certain. It appeared as if this was a request to increase activities.

Senator MONDALE. Could you tell the committee what kinds of things you would expect to follow had the Huston plan been approved, in terms of the use of the NSA?

Mr. BUFFHAM. I don't think we ever made an analysis of that, Senator.

Senator MONDALE. But you indicated you were concerned about what would be expected of you—the degree to which you would have to go beyond your current practices—should the Huston plan be approved. Can you tell us what things concerned you?

Mr. BUFFHAM. Well, remember there was a lot of confusion on this particular item.

The committee, which Admiral Gayler was a member of, was tasked to draw up a plan, not a plan, it was tasked to draw up an analysis of what kind of foreign threat existed and where there were gaps in intelligence and they were not asked to make any recommendations, they were merely asked to identify gaps and to suggest various alternatives which could remedy possibly that gap.

Senator MONDALE. One of the remedies suggested was to greatly broaden the authority of the NSA to intercept messages.

Mr. BUFFHAM. That was one of a series of alternatives under that particular item. There was no recommendation made by Admiral Gayler or any members of that Ad Hoc Intelligence Committee. What happened was that after the committee's report went to the White House, Mr. Huston analyzed all of the alternatives and he selected those which, in his judgment, he felt the President should approve. And he then prepared a memorandum to the President through Mr. Haldeman, which was approved and then later, withdrawn and rejected and never implemented. But those were Mr. Huston's ideas of what should be done.

Senator MONDALE. What did Mr. Huston have in mind? Had this approval been given to the NSA?

Mr. BUFFHAM. That I do not know, sir.

Senator MONDALE. You have no idea whatsoever? I am told this option was submitted by the NSA.

Mr. BUFFHAM. No. This was one of three or four alternatives drawn up under that particular item.

Senator MONDALE. Did the NSA want it? Did Admiral Gayler oppose it?

Mr. BUFFHAM. Admiral Gayler did not want it, to my knowledge.

Senator MONDALE. He opposed it? Is there anything in writing suggesting—

Mr. BUFFHAM. He was specifically asked, as all the members of the committee were asked by Huston, not to make recommendations, but merely to specify alternatives. But the determination as to what alternative, if any, was to be selected was to be a White House matter. Now, the only exception to that was that Mr. Hoover, after the report had been signed by the other members, he gave his personal views as to what should be done with those various alternatives, and that was not checked with the other members of the ad hoc committee report.

In other words, Admiral Gayler did not know that Mr. Hoover was going to submit separate comments, and Admiral Gayler did not submit separate comments himself; because it was his understanding, as it was all of us that were involved in that exercise, that that was not what was required or desired.

Senator MONDALE. Mr. Buffham, is it your testimony that you do not have any idea what Mr. Huston had in mind by the option which we are discussing; namely, to greatly broaden the discretionary authority of the NSA?

Mr. BUFFHAM. Well, I don't know positively. But I would assume that he would have thought that the other intelligence agencies would then increase the numbers of names on their lists, and ask NSA to do something by way of specifically targeting those people, including for collection. And that was not a practice that was done then or ever has been done by NSA.

Senator MONDALE. It was one that concerned you a great deal?

Mr. BUFFHAM. Yes; it concerned all of us in the NSA.

Senator MONDALE. Were you concerned about its legality?

Mr. BUFFHAM. Legality?

Senator MONDALE. Whether it was legal.

Mr. BUFFHAM. In what sense; whether that would have been a legal thing to do?

Senator MONDALE. Yes.

Mr. BUFFHAM. That particular aspect didn't enter into the discussions.

Senator MONDALE. I was asking whether you were concerned about whether that would be legal and proper.

Mr. BUFFHAM. We didn't consider it at the time; no.

Senator MONDALE. But at least you would not do it without the President's direct authority.

Mr. BUFFHAM. That is correct.

Senator MONDALE. All right.

May I ask one more question of the General Counsel? In your opinion, was the watch list legal?

Mr. BANNER. I think it was legal in the context of the law at the time.

Senator MONDALE. Has any law changed that legality?

Mr. BANNER. Well, we have since had decisions such as in the *United States v. U.S. District Court* case in 1972 which placed—which stated in effect that the President does not have the authority to conduct a warrantless surveillance for internal security purposes.

The CHAIRMAN. May I just suggest that in line with my earlier statement, it seems to the committee that the Attorney General of the United States should be asked about the legal and constitutional questions that are raised by the disclosures this morning. I do not mean to cut you off, Senator.

Senator MONDALE. I will live with that. But what I was trying to demonstrate is what I think the private record discloses; that they thought that to be legal. I think that is important to the determination of this committee of how these laws are interpreted. I believe they still think it is legal. That is what worries me.

Mr. BANNER. May I make just one comment, Mr. Chairman? There is one court decision on the matter. It was held in that decision to be lawful.

Senator MONDALE. Then you think it is lawful? That is what it held?

Mr. BANNER. I think it was lawful at the time.

Senator MONDALE. That is my point. They still think it is legal.

Senator MORGAN. Mr. Chairman, could we ask him to give us a decision some time?

Senator GOLDWATER. He said it was lawful at the time.

The CHAIRMAN. I think all relevant decisions on the matter should be supplied by the General Counsel of the Agency. But we will look, in the main, to the Justice Department on these legal questions.

General, thank you very much for your testimony. If there are no further questions, you are excused at this time.

The CHAIRMAN. Now we have another matter that needs to be brought up before the public hearing concludes this morning, and I will speak of it just as soon as these gentlemen have an opportunity to depart.

Please come back to order. At the outset this morning, I mentioned that this hearing would be conducted in two parts. The reason for doing so has been made evident in the course of the proceedings. Although the administration had objected to a public hearing on any matter relating to the NSA, the committee, by majority vote, believed that it was necessary to bring the facts relating to the watch lists to the attention of the American people through a public hearing. As I mentioned earlier, though the administration opposed the hearing, it did cooperate to the extent of declassifying the materials, and consenting to General Allen's appearance as a witness. Now, we come to the second part, another matter that the committee must decide upon to which the administration has given no consent either to furnish witnesses or to declassify materials.

Senator Goldwater, I think, had special reference to this second aspect.

Senator GOLDWATER. It does, but I would like to correct the record. We did not take a vote on this subject.

The CHAIRMAN. Yes; in executive session yesterday, with a quorum present, the procedures which we have followed today were presented and approved without objection. And I took that to mean, in accordance with normal procedure, that the committee had given its consent.

Senator GOLDWATER. I left a note to be recorded against it, and I had assumed a vote would be taken. But it was not.

The CHAIRMAN. Well, had a vote been taken, or anyone on the committee had moved to take a vote, Senator, your objection would have been recorded as you requested.

Now, in connection with the second matter, I would like first to respond to some of the questions that were raised earlier by Senator Goldwater with respect to the legality of our making a public disclosure of the second subject. I personally have no problem with the legality of doing so. The Constitution of the United States provides, in article I, section 5, clause 2, that each House may determine the rules of its proceeding; and in clause 3, that each House shall publish its proceedings, except parts as may, in their judgment, require secrecy.

This committee was empowered by a resolution of the Senate to inquire into this subject matter, including the NSA. And that resolution, S. Res. 21, gives the committee the power to pass such rules as it may deem necessary on disclosure, and makes clear that the committee rules can authorize disclosure. So that the rules are based solidly on S. Res. 21, the underlying resolution by which the committee was created.

Senator GOLDWATER. Would the Senator yield?

The CHAIRMAN. If I may just complete the—

Senator GOLDWATER. I wish you would read section 2 of that also.

The CHAIRMAN. Yes, I will. I was just getting to the Senate rule, and I will read it all. In pursuance of S. Con. Res. 21, the committee adopted its rules, and the relevant rule is section 7. Section 7.5 is the relevant rule. If counsel will find it for me, I will read it. It reads:

No testimony taken, including the names of witnesses testifying, or material presented at an executive session, or classified papers or other materials received by the staff or its consultants while in the employ of the Committee, shall be made public in whole or in part, or by way of summary, or disclosed to any person outside the Committee, unless authorized by a majority vote of the entire Committee; or after the determination of the Committee in such manner as may be determined by the Senate.

So, it appears to me that making a public disclosure of the matter now under consideration is subject to the will of this committee; and I would like to read into the record the reasons why I believe such a public disclosure should be made; after which I will invite Senator Tower, who disagrees with me on this subject, to express for the record the reasons why he thinks such a disclosure should not be made.

It being 25 minutes of 1 now, Senator, it may not be possible for this whole matter to be discussed or debated. But if it cannot be resolved at this time, it will be taken up in the next session of the committee this afternoon, and with the hopes that the committee can then reach a final determination by vote.

Senator TOWER. Mr. Chairman, if you would yield at that point.

The CHAIRMAN. Yes.

Senator TOWER. I will state my reasons briefly at the conclusion of your remarks. Obviously, it is difficult to pursue the matter in open session, because those who oppose disclosure have some difficulty in explaining the reasons why in an open session.

The CHAIRMAN. And for that reason, I will certainly accommodate the request in the interest of fairness, so that there can be a full and complete discussion within the committee and the vote then can be taken by the committee. That, I would anticipate, would occur this afternoon when the committee goes into executive session.

The reasons why I believe that this second matter should be made public are as follows. This committee has proceeded with great caution

throughout its investigation, which has covered a broad range of NSA activities. Testimony has been taken from numerous NSA officials, all in executive session until this morning. The committee has also received extensive briefings from General Allen and others in private.

Most of these activities we have found to be legitimate, clearly within the scope of the intelligence purposes of the agency, and for reasons that the committee feels relate to sensitive national security matters, should be kept secret. But our investigation did uncover two NSA activities which I believe are properly subject to some form of public disclosure. Because, one, they would appear to be unlawful; two, they have now been terminated, and thus do not represent ongoing activities; three, they can be discussed without revealing the NSA's sensitive techniques; and four, legislation is needed to prevent their repetition. What has occurred yesterday could occur tomorrow, if we leave it all to executive decision.

Now, as I have said, as to one of these—the watch list—the administration agreed to declassify the documents, and authorize General Allen to testify as he has. As to the other, the executive branch has consistently opposed public hearings or any other form of public disclosure. Yesterday, the committee, in the manner I described in response to Senator Goldwater, agreed that we nevertheless would disclose facts concerning the second program to the American public.

I believe that the public is entitled to an explanation of why that decision was made yesterday, in face of the administration's strongly stated opposition. I do not suggest that the administration has acted in any way other than in good faith to exercise its responsibilities as it perceives them. However, Congress has a right and duty to exercise some judgment on its own. It must do so fairly, properly, and with due regard to the views of the executive. But it cannot simply abdicate to the executive.

We believe that—or at least let me speak for myself—I believe that yesterday's decision does represent a proper exercise of the constitutional responsibility of the committee, which is charged with an investigation of this importance, and charged by the legislative branch to perform it. As I understand it, the executive branch makes two arguments, which were stated often in executive sessions of the committee, against a public disclosure of this second matter. Neither of them, as I heard the many spokesmen who came up to present them, made any particular point of sensitive technology, or anything of a character that would reveal the nature of NSA's operations. Their arguments seemed, rather, to focus first on their concern that the disclosure of the identity of certain companies and activities would make other companies hesitate to cooperate with our intelligence agencies in the future; and second, that such a disclosure might be of embarrassment to the particular companies concerned.

I believe that the answer to the first argument is that companies should hesitate to comply with requests of the Government at least long enough to determine if the actions they are requested to do are lawful and do not violate the constitutional rights of American citizens. And I believe the answer to the second argument is that fairness to the companies themselves requires that the facts be fully and fairly stated, which I think this committee is in a position to do.

I believe that it would be inappropriate to keep secret the facts of this second program, since in my judgment they establish apparent violations of section 605 of the Federal Communications Act, and of the fourth amendment to the Constitution. Second, the program involved neither ongoing activity nor technological secrets. And third, exposing it is directly related to whether the NSA needs a legislative charter to govern and control its activities in the future. Finally, the public debate that we hope will ensue from this session may make both the Government and private companies more careful to weigh the legality of programs that may be suggested in the future.

So in balancing the arguments for and against disclosure, which we have done most carefully, we have consulted extensively with the executive branch. Several times we have delayed our action to make certain that we had heard all of the executive branch's arguments. We have engaged in extensive interrogations of General Allen and Director Colby and the Secretary of Defense, Mr. Schlesinger, and finally, from the Attorney General and representatives of the President. So we believe we have listened fully to the arguments that they wish to present.

If the committee remains firm in its decision, the second matter is what form of disclosure would be most appropriate. Since witnesses have not been made available by the executive branch, it seems to me that the most appropriate form of disclosure would be that of a statement issued on the authority of the committee itself, carefully drawn to present the key facts unemotionally and without fanfare. As to the accuracy of the statement, it would be carefully checked with the Agency itself so that there would be no factual distortions in the presentation. The statement, I might emphasize, would be based on testimony received by the committee in executive session. It would not quote in whole or in part from the text of any classified document presented by the executive branch to the committee. Because the testimony given in executive session before this committee was classified by the committee itself, pursuant to the committee's rules, the committee has every right to release such facts based upon such testimony. Indeed, it has the right to release the testimony itself should it so decide.

So the decision taken yesterday to release this information was based primarily on the belief that programs of such dubious legality should be disclosed; because, absent real national security factors, which are not present in this case, classification should not be used to hide or cover wrongdoing. And, as I have said, in the technical sense, I do not think that classified information is being released at all.

The decision to make this matter public should, in my view, be tested not only against its particular facts but also in the light of several general principles. First, in a democratic society, there should be a strong preference in favor of letting the people know what their Government has been doing. Democracy depends upon an informed electorate. As one of our Founding Fathers, Edward Livingston, stated:

No nation has ever found any inconvenience from too close an inspection into the conduct of its officers, but many have been brought to ruin and reduced to slavery by suffering gradual impositions and abuses which are imperceptible, only because the means of publicity had not been secured.

Second, the general principle for disclosure is particularly apt in the context in which this committee finds itself. For 30 years this

country has had a huge and highly secret intelligence apparatus whose actions have not been the subject of an informed public debate. Laws governing their activity have all too often been lacking, as with the NSA, or overly vague, as with the CIA. The agencies have sometimes acted in ways that appear to be unconstitutional and illegal. The Congress and the public should now be given a chance to decide whether changes in the laws and procedures governing the intelligence agencies are necessary. That has not happened for 30 years, and surely we can afford a debate at least once in a generation.

Third, it does not follow, of course, that everything we learn in the work of this committee should be disclosed. And from what I have previously said, much of what we have learned about the NSA, which, in the judgment of the committee, falls clearly within its province, will not be disclosed. This country should have strong and effective intelligence services, but we must act legally. Keeping unlawful programs secret can only serve in the long run to weaken our intelligence efforts.

Unless the people are convinced that the intelligence agencies are acting within the law and in the best interests of the United States, a democratic people will not support these agencies for long. "Eternal vigilance," as Thomas Jefferson said, "is the price of liberty." And as James Madison concluded, "the right of freely examining public characters and measures and the free communication thereon is the only effective guardian of every other right." For these reasons, I believe that it would be proper for the committee to approve the disclosure of the second matter to which the discussion relates.

Now, I defer to Senator Tower.

**Senator TOWER.** Thank you, Mr. Chairman.

Mr. Chairman, I was unavoidably absent from the meeting yesterday in which, without objection, it was decided that this matter would be spread on the public record today. Had I been there, I would have objected, and perhaps this debate could have ensued at that point. My justification for not being there is that I am the ranking minority member of the Banking Committee which was at that moment considering the plight of New York City. So I was buried in the bowels of the fiscal mismanagement of that great city, and I am sorry that I was not there.

I really see no legislative basis for this public disclosure. I do not think it is necessary, from the standpoint of our legislative mandate. It appears that Committee Rule 7.5 is the only point having any merit at all. And in my view, it must fail. This rule provides for procedures insuring the protection of classified materials. This rule does not authorize the unilateral release of classified information. A proper reading would be that the rule goes to disclosure of information, not declassification. A majority vote is necessary prior to committee release of any material of a classified nature. But it is spurious to state that a simple majority vote is enough to declassify a document or information, an action which I do not believe has before been recognized as a congressional prerogative.

Let me read from the resolution, which I believe is superior to any rule that we may adopt:

The Select Committee shall institute and carry out such rules and procedures as it may deem necessary to prevent the disclosure outside the Select Com-

mittee of any information which would adversely affect the intelligence activities of the Central Intelligence Agency in foreign countries or the intelligence activities in foreign countries of any other department or agency of the Federal government.

At this point, I read into the record a note from Mr. David D. Lowman, Special Assistant to the Director, NSA, for Congressional Review, to Mr. Barry Carter of the Select Committee staff.

Barry, we have reviewed Senator Church's proposed statement on SHAMROCK. With the exceptions noted here previously, the statement is essentially correct. After reviewing the document, we have concluded that, since it does reveal sources, methods and capabilities, its classification should be Secret, Handle via COMINT Channels Only.

It is my view that it is not necessary for us to make this matter public. Therefore, we should not, by virtue of the risks that we run in doing so. It occurs to me that today's disclosure, should we do so, would be cited in some future date as a precedent to allow each Member of Congress and committee the right to decide what should be publicly available from what the executive branch has determined to be secret. This would mean revelation through public channels to our enemies and would lead to chaos and ultimately destruction of the very fragile intelligence effort.

President Truman decided that this matter should be kept secret. President Ford has personally and specifically requested of the committee that it be kept secret. Of course, a Member of the other body has threatened to make this matter available to the public before we have acted on it. I do not think we should rush to do the same. I think, quite to the contrary, we should implore the House not to. I think one Member out of 435 in the House of Representatives should not be encouraged to reveal matters that impact on the lives and safety of the people in the other 434 congressional districts in this country. They have a stake in this matter, too.

Now, I think that if this information is released, as the chairman has proposed, the ripple effect will seriously impair the confidence that other nations have in dealing with us, impact on the efficacy of Strategic Arms Limitation Agreement, progress in mutual balance of force agreements, nonnuclear proliferation arrangements. Already the intelligence services of other countries are showing some indisposition to cooperate with the United States, for fear that their own methods, their own resources, their own activities, to the embarrassment of their respective governments, or to the detriment of their intelligence-gathering capability, will be affected. For these reasons, Mr. Chairman, I urge that this matter of the details of the SHAMROCK operation not be made public. I would urge the members of the committee to reconsider the decision of yesterday in an executive session.

The CHAIRMAN. Thank you, Senator Tower.

Before we close, are there any other comments?

Senator Mondale.

Senator MONDALE. Mr. Chairman, I just wanted to comment briefly on what I thought I heard to be the argument, that somehow the classification and determination of the executive department should govern how this committee decides to release or not to release information to the public. I do not think we can accept that definition for a moment. If we do, I think we are no longer a coequal branch of Government.

We have just been through one of the most dispiriting periods of American history, and the defense that was always raised, every time you wanted to find out about it, was national security. So it seems to me there are occasions when the national security interests clearly dictate and require secrecy. And there are instances when national security is raised, not to protect this Nation's security, but to protect some contemporary politicians from embarrassment. It is our job, as Members of the Congress, to decide where that line is and to do so with a firm notion of our sacred responsibility not only to investigate but to inform the public.

I am glad that it has been decided that we will hold this debate in private. I think it ought to be thoroughly aired, but finally, it is our responsibility as members of the Senate and of this committee to make our own determination as to whether or not these matters, if disclosed, would undermine the Nation's security. I look forward to that argument.

But I did want to say that I do not think for a moment that we can accept the simple declaration by the Executive that it is classified, as precluding or undermining our capacity to make an independent judgment.

The CHAIRMAN. Thank you, Senator.

I agree with that. I think we would be a prisoner of the Executive if we took such a position.

Senator TOWER. May I say, Mr. Chairman, that I have been co-operative, I believe, and have supported every effort to obtain the documents that we require. That is one thing. I believe that we should have those documents. We should have access to them; we should have access to witnesses, and we should be fully informed, and we should make thorough investigations.

The question here is whether or not this information should be made public. Yes, there is a right of the people to know, but that must be balanced against the fact that when these matters are made public record, they are available also to our enemies. Let me cite one example. A weekly magazine published the fact that we had been reading the telemetry on Russian weapons systems from Turkey. As soon as that matter was made a matter of public record, it was also available to the Soviets, and that source was then and thereafter denied us. This impacts on our capability for verification in terms of strategic arms capabilities and deployment. I do not think that the public interest was served in the release of that information. Indeed, it was not served. So I think there are some very strong examples that can be cited.

I appreciate the chairman's disposition to take this matter up in executive session and, hopefully, I can prevail there. I have no illusions about these matters.

The CHAIRMAN. Well, I think the Senator always states his case with great authority and has persuaded the committee on occasion. I hope he will not persuade the committee on this occasion, because the examples he gives that are so terrifying have nothing to do with the case at hand, which relates to quite a different matter.

Senator TOWER. Yes, they do, because we are talking about people's rights to know here.

The CHAIRMAN. I think what we are talking about—

Senator TOWER. I think it is proper to cite examples of where that right can be subordinated.

The CHAIRMAN. Of course, Senator, when you cite your examples, who would argue with them? But the case at hand has to do with unlawful conduct that relates to certain domestic companies in this country. And it is not a matter of such gravity that it would even impair the national security of the United States—

Senator TOWER. Well—

The CHAIRMAN. In ways that your examples suggest.

Senator TOWER. That is a matter to be debated in executive session.

The CHAIRMAN. Yes. Very well, we will debate it in executive session.

Senator TOWER. There is more to be said then.

The CHAIRMAN. A good deal.

Senators who wish to be heard; I want to recognize first—Senator Morgan wants to be recognized. First, let me recognize Senator Baker.

Senator BAKER. Mr. Chairman, thank you. I will not take very long. I simply want to say, as a matter of legal argument, that the rules of this committee can be no broader nor create any authority and jurisdiction beyond the rules of the Senate from which we derive our authority, and it seems to me that the rules of the Senate, at least arguably, say that a classified document cannot be declassified or released to the public without the prior consent of the executive department, or at least, not without changing the rules of the Senate itself. So the argument that our committee rules give us that authority by majority vote, I think must be tempered by the preposition that the committee rules are subordinate to and can be no greater than the rules of the Senate itself, which appear to say something else.

Beyond that, as the chairman knows, and as I believe other members of the committee know, I have sometimes been the only member of the committee, always, however, in a minority, who has contended that all of our proceedings should be in public, and I am rather perturbed really, that we are about to go into executive session on this matter and to deal with only just a report. I am rather perturbed rather that we are going into public session instead of executive session, when you compare the relative potential for harm, the relative comparison for the potential for embarrassment in the case of the assassination plots, which were some time ago, versus the potential for destruction of intelligence sources and methods when we are dealing with an ongoing program today. In a word, if you are going to have public hearings on NSA, you sure should have had them on assassinations because I think assassinations are far less sensitive, in term of the welfare of this country, than the NSA situation is, the SHAMROCK situation.

Now, Mr. Chairman, I think that the proper course for us to take and the course we will, no doubt, debate in executive session this afternoon, is to try to gain access to as much information as we can and to obtain the concurrence of the executive department on as much information as we can before we proceed then to public hearings. I favor public hearings. I do not, however, favor public hearings until we have exhausted every opportunity to obtain the declassification of as much information as possible. I will oppose the unilateral declassifi-

cation by this committee of this information, which I am afraid is the sum total and the functional effect of what is being proposed.

The CHAIRMAN. I thank the Senator. I know his position on public hearings, but frequently in executive session, he has voted against them on the grounds that we were not adequately prepared.

Senator BAKER. No, I have not.

The CHAIRMAN. I think in this case we are very adequately prepared because we have had all kinds of executive hearings, and we have heard the executive agencies and their spokesmen again and again relating to all the particulars of this particular subject.

Senator BAKER. Mr. Chairman, if I understand you correctly, I believe you said that in executive session I had voted against public hearings. I do not believe the record will disclose that. I think the record will disclose that I voted against declassifying or proceeding with a particular piece of information. I do not believe the record will show that I voted against public hearings on any issue.

The CHAIRMAN. The record can speak for itself, but in any event, I have heard the Senator make the argument before in connection with public hearings that we were not prepared.

Senator BAKER. And I persist in the hope that someday I may prevail.

The CHAIRMAN. I do not know what more exhaustive preparation could have been laid than the one that has been laid for the matter now before the committee. Senator Morgan.

Senator MORGAN. Mr. Chairman, I would not want to go away from here with anyone having the misunderstanding that information has been withheld from this committee.

As General Allen testified this morning—and that is correct according to my knowledge—he has furnished to us all of the information that we have asked for and has indicated his willingness to furnish it to us. The thing that concerns me—and I was in and out of the meeting yesterday afternoon. Like Senator Tower, I had to be on the Banking Committee and on the floor—the thing that concerns me is so many people express their concern about going public with this hearing after we have been able to work out almost every difficult situation in the past.

I know from your own statements that the President himself has personally intervened with you or talked with you. No later than this morning he talked with me about it again through his emissary. He has expressed his concern. I have a great deal of confidence in the President. I think we ought to pass judgment on it ourselves, but I just would want the record to reflect that nobody is withholding information from this committee. There is one other thing I think Senator Tower's comments pointed out—the danger of going public. A couple of times Senator Tower referred to a couple of things that, so far, maybe we should not refer to, but since he referred to President Truman, let me say President Truman long, long ago was involved in this and gave his word and, because of it, I am awfully reluctant to go against the word of the President of the United States. If we cannot depend on the word of the President of the United States, I do not know who else the American people can look to.

The CHAIRMAN. Well, I think just to complete that since the Senator has stated it, President Truman also said that his word would not

be binding. He could not bind future administrations. So I really believe that was a long time ago and the commitment was one that he, himself, put a condition on, and moreover the program changed. It changed greatly after the original agreement was entered into.

So, anyway, this is a matter for executive debate.

Senator GOLDWATER. Mr. Chairman, I want to emphasize that had we known that this subject was going to be decided yesterday, I would have stayed away from the floor, where I had to be to engage in a debate on the promotion of an Air Force General, and these other gentlemen would have been there, too. I do not even know if there was a quorum present, but the rule calls for a majority vote, and I do not believe the question was ever put, so that the answer could have been from the Chairman by unanimous consent it is agreed. I have not found a member yet that could substantiate that kind of a move, so we have not voted on this. In fact, as I recall it, we have only had a couple of votes in the whole history of this Committee.

The CHAIRMAN. Well, Senator, it is clear that this will be debated once more in executive session and will then be voted, so there will be no basis for a complaint that the rules have not been completely, faithfully, and scrupulously adhered to.

If there is no further comment, this public session is now adjourned.

[Whereupon, at 1:07 p.m., the committee recessed, subject to the call of the Chair.]

# INTELLIGENCE ACTIVITIES—THE NATIONAL SECURITY AGENCY AND FOURTH AMENDMENT RIGHTS

---

THURSDAY, NOVEMBER 6, 1975

U.S. SENATE,  
SELECT COMMITTEE TO STUDY GOVERNMENTAL OPERATIONS  
WITH RESPECT TO INTELLIGENCE ACTIVITIES,  
*Washington, D.C.*

The committee met, pursuant to notice, at 10:05 a.m., in room 318, Russell Senate Office Building, Senator Frank Church (chairman) presiding.

Present: Senators Church, Tower, Huddleston, Hart of Colorado, Goldwater, Mathias, and Schweiker.

Also present: William G. Miller, staff director; Frederick A. O. Schwarz, Jr., chief counsel; Curtis R. Smothers, counsel to the minority; and Charles Kirbow, professional staff member.

The CHAIRMAN. The committee will please come to order.

Last week, it will be remembered, a question developed over whether or not the committee should make a public disclosure on one operation that had been conducted in the past by the NSA. The committee took that question under advisement and had the statement that it was proposed for the chairman to read, carefully checked for accuracy, and carefully checked to make certain that it would reveal no method or technology that would be harmful to the intelligence operations of the United States. The committee then voted on Monday, November 3, by a vote of seven to three, that the information should be made public, subject to confirmation by the Senate Parliamentarian that doing so would not constitute a violation of the Senate rules. The committee received such confirmation from the Parliamentarian yesterday and that was read to the committee in the session yesterday afternoon.

The reasons, it seems to me, for the disclosure are clear. The program certainly appears to violate section 605 of the Communications Act of 1934, as well as the fourth amendment of the Constitution. That program has been terminated as of now, and the statement to be given today does not divulge technology or sensitive intelligence methods. Indeed, no particular technology was ever involved in the procedure that was used. It amounted to a simple turnover of telegraph traffic to the Government.

The committee believes that serious legal and constitutional questions are raised by this program. For that reason, the committee voted to disclose it. The following statement is the one that has been reviewed by the committee and voted on for disclosure this morning.

SHAMROCK was the cover name given to a message-collection program in which the Government persuaded three international telegraph companies, RCA Global, ITT World Communications, and

Western Union International, to make available in various ways certain of their international telegraph traffic to the U.S. Government. For almost 30 years, copies of most international telegrams originating in or forwarded through the United States were turned over to the National Security Agency and its predecessor agencies.

As we discuss more fully below, the evidence appears to be that in the midst of the program, the Government's use of the material turned over by the companies changed. At the outset, the purpose apparently was only to extract international telegrams relating to certain foreign targets. Later, the Government began to extract the telegrams of certain U.S. citizens. In defense of the companies, the fact is that the Government did not tell them that it was selecting out and analyzing the messages of certain U.S. citizens. On the other hand the companies knew they were turning over to the Government most international telegrams, including those of U.S. citizens and organizations. There is no evidence to suggest that they ever asked what the Government was doing with that material or took steps to make sure the Government did not read the private communications of Americans.

The select committee made its first inquiries into this operation last May. It was not until early September, however, that the select committee received a response to its questions. At that time, we obtained preliminary briefings from NSA operational personnel. Subsequently, we examined three NSA officials, including former Deputy Director Louis Tordella. These persons were the only ones at NSA with substantial knowledge of the SHAMROCK operation. The committee also reviewed all existing documentation relating to the operation. The select committee again examined NSA officials in executive sessions. Subsequently, the companies which had participated were contacted. Sworn testimony was taken from officials in each company, and company counsel have worked with the committee to reconstruct, as nearly as possible, what has taken place over the last 30 years.

During World War II, all international telegraph traffic was screened by military censors, located at the companies, as part of the wartime censorship program. During this period, messages of foreign intelligence targets were turned over to military intelligence.

According to documents in possession of the Department of Defense, the Department sought in 1947 to renew the part of this arrangement whereby the telegraph traffic of foreign intelligence targets had been turned over to it. At that time, most of these foreign targets did use the paid message facilities of the international carriers to transmit messages.

At meetings with Secretary of Defense James Forrestal in 1947, representatives of the three companies were assured that if they cooperated with the Government in this program they would suffer no criminal liability and no public exposure, at least as long as the current administration was in office. They were told that such participation was in the highest interests of national security.

Secretary Forrestal also explained that the arrangements had the approval of President Truman and his Attorney General, Tom C. Clark. Forrestal explained to the companies, however, that he could not bind his successors by these assurances. He told the companies, moreover, that Congress would consider legislation in its forthcoming session which would make clear that such activity was permissible. In fact, no such legislation was ever introduced.

In 1949, the companies sought renewed assurances from Forrestal's successor, Louis D. Johnson, and were told again that President Truman and Attorney General Clark had been consulted and had given their approval of these arrangements. As I will explain later in this statement, neither the Department of Defense nor any of the participating private companies has any evidence that such assurances were ever sought again.

The Army Security Agency (ASA) was the first Government agency which had operational responsibility for SHAMROCK. When the Armed Forces Security Agency was created in 1949, however, it inherited the program; and, similarly, when NSA was created in 1952, it assumed operational control.

There are no documents at NSA or the Department of Defense which reflect the operational arrangements between the Government and the telegraph companies. The companies decided at the outset that they did not want to keep any documents, and the Government has none today other than those relating to the 1947 and 1949 discussions which I previously covered.

According to the testimony given to us, it appears, however, that the companies were given to understand at the outset that only traffic of foreign intelligence targets would be gleaned by NSA. In practice, the arrangements with each company varied somewhat. RCA Global and ITT World Communications provided NSA with the great bulk of their international message traffic, which NSA then selected for traffic of foreign intelligence targets. Western Union International sorted the traffic itself and provided NSA only with copies of the traffic of certain foreign targets and all the traffic to one country.

In the beginning, the Government received paper tapes of messages that had been transmitted by overseas cables, as well as microfilm copies of messages that had been sent by radio. These were, at the outset, sorted by hand apparently for certain foreign intelligence targets only; such traffic could be readily identified by special codes in the heading of each telegram. As a practical matter, the inherent limitations of manual sorting precluded the traffic from being sorted on its content.

In the early 1960's, there was a change in technology which had a significant impact upon the way in which SHAMROCK was run. RCA Global and ITT World Communications began to store their international paid message traffic on magnetic tapes, and these were turned over to NSA. Thereafter, the telegrams were selected in precisely the same way in which NSA selects its information from other sources. This meant, for example, that telegrams to or from, or even mentioning, U.S. citizens whose names appeared on the watch list in the late sixties and early seventies, would have been sent to NSA analysts, and many would subsequently be disseminated to other agencies.

The NSA officials examined by us had no recollection of NSA's ever informing the companies how NSA was handling the information they were providing. They furthermore had no recollection of any of the companies making such an inquiry, even after NSA began receiving magnetic tapes from two of the companies. Several company officials corroborated this testimony, stating that they had no knowledge of any inquiry by their respective companies or that NSA ever volunteered any information in this regard.

Only the Director, Deputy Director, and a lower-level manager at NSA had operational responsibility for SHAMROCK at any one time. Moreover, their contacts with company officials were extremely rare; in fact, the Director never met with company representatives and the Deputy Director only met once with a company official. Any communications with the companies were usually relayed by NSA couriers who made routine pickups and deliveries at the companies.

No one examined from NSA or the companies knew of any effort by the companies since 1949 to seek renewed assurances from the Government for their continued participation in SHAMROCK. Indeed, each of the companies has given sworn statements to the committee that they did not think the arrangements with NSA were ever considered by the executive levels of their respective companies. Moreover, Dr. Tordella, the former Deputy Director, told us that he would have known if additional assurances had ever been sought and testified that to his knowledge they were not.

NSA and company officials likewise knew of no compensation given the companies by the Government for their participation in SHAMROCK, and testified that they knew of no incident where favoritism was shown any of the participating companies by an agency of the Federal Government. Again, Dr. Tordella has stated under oath that he would have been told about such an incident if it had taken place.

NSA never received any domestic telegrams from these companies. Indeed, none of these companies, at least since 1963, has had domestic operations.

Approximately 90 percent of the messages collected in SHAMROCK came from New York. Company offices in Washington, San Francisco, and, for a short while, Miami, also participated in a similar fashion. In Washington, the companies turned over copies of particular traffic intelligence targets to agents of the FBI. These were later delivered to NSA.

Of all the messages made available to NSA each year, it is estimated that NSA in recent years selected about 150,000 messages a month for NSA analysts to review. Thousands of these messages in one form or another were distributed to other agencies in response to "foreign intelligence requirements."

Until the current controversy arose, only a handful of officials in the executive branch over the last 30 years were apparently aware of the SHAMROCK operation. Dr. Tordella testified that to the best of his knowledge no President since Truman had been informed of it.

SHAMROCK terminated by order of the Secretary of Defense on May 15, 1975.

Senator TOWER. Mr. Chairman.

The CHAIRMAN. Senator Tower.

Senator TOWER. Thank you, Mr. Chairman.

Although I have consistently endorsed the aims and efforts of this committee and have pledged myself to an exhaustive and responsible evaluation of all aspects of our intelligence community, I must state my firm opposition to this unilateral release of classified information. I am greatly concerned that any unwarranted disclosures could severely cripple or even destroy the vital capabilities of this indispensable safeguard to our Nation's security.

Despite the very best intentions of this committee, and despite its established record of sensitivity to the delicate nature of national security, I cannot assent to its decision to declassify information whose disclosure the Director of NSA has consistently asserted would hamper the NSA mission.

The NSA has furnished the staff in executive session with all requested documents and information. General Allen and his colleagues repeatedly made good their promise to keep this committee fully informed. They have comprehensively briefed this committee in executive session and have answered all our requests and questions. I simply see no purpose to selected release of classified matters about which we have already been fully briefed, thereby running the very real risk of compromising the work of this extremely important, but exceptionally fragile agency.

I say again, the public's right to know must be responsibly weighed against the impact of release on the public's right to be secure.

I must therefore take strong exception to the action this morning which, in effect, unilaterally releases classified information. Such a decision does not comport with the stated aims of this committee, nor further the objectives of this investigation. Indeed, it may very well contravene the resolution establishing this committee by improperly promoting disclosure outside the select committee of information which would adversely affect our intelligence activities in foreign countries.

Therefore, I voice my concern and my dissent.

**Senator GOLDWATER.** Mr. Chairman.

**The CHAIRMAN.** Senator Goldwater.

**Senator GOLDWATER.** Mr. Chairman, I support the statement of the vice chairman. I was one of the three in the committee that voted against releasing the SHAMROCK information. I believe the release of communications intelligence information can cause harm to the national security; moreover it can lead to serious diplomatic problems with our allies.

The committee has all the information it needs to recommend legislation on communications intelligence, and I believe we ought to get on with the job. Up to now this committee has had a very commendable record for maintaining secrecy, and I hope we are not going to stray from that good course. The fact that the other body, the House, seems to be irresponsible in its treatment of the subject is no reason in my opinion for the Senate to try to use that as an excuse for disseminating secret material, nor to try to copy irresponsibility.

The American people expect the Congress to take remedial action when necessary. The American people also expect the Congress to act responsibly in maintaining our national defense.

**The CHAIRMAN.** Are there any other Senators who would like to comment? Senator Huddleston.

**Senator HUDDLESTON.** Mr. Chairman, just very briefly to comment on the action of the majority of the committee in releasing this report. This is certainly the kind of judgment that this committee has had to make on numerous occasions since the beginning of our inquiry. I might say prior to this decision there was a great deal of effort, a great many meetings between the NSA, the White House, the com-

mittee members, and the committee staff as to just precisely how the people's right to know might be balanced with the need for security.

I believe the manner in which this has been done has revealed to the public certain elements of activities that might be considered to be incorrect. I do not see how you can pass legislation in a vacuum. I believe that there has to be a certain amount of knowledge made available to the public and made available to the Congress before reasonable and meaningful legislation can be processed. I believe that this has not in any way jeopardized or compromised the security of our country or the activity of the NSA or other intelligence gathering agencies of our Nation, that they can go forward just as effectively, perhaps more so, following the result of action of this committee in developing the proper guidelines and proper procedures for our entire intelligence organization's policy.

Thank you, Mr. Chairman.

The CHAIRMAN. Thank you, Senator Huddleston.

Senator Hart.

Senator HART of Colorado. Mr. Chairman, I agree with the action taken here this morning, even though, as you know, I was one of those who originally opposed public hearings on this matter.

This project involved soliciting and obtaining cooperation of certain international telegraph companies in providing large volumes to the Government for nearly 30 years, in some cases all of the international traffic passing over their facilities. Project SHAMROCK is improper it seems to me for many reasons, including, first, that it appears unlawful under section 605 of the Communications Act of 1934, and the fourth amendment, although there is no case exactly in point. Second, it placed the Government in a position to request illegal acts of the companies, contrary to the proper role of the executive to see that the laws are faithfully executed. Third, it resulted in the Government promising the companies immunity from criminal prosecution to obtain the cooperation. It raised the possibility which did not occur insofar as our effort shows, that the companies might some day terminate their participation unless the Government granted some benefit, withheld some penalty, or halted some investigation. It resulted in the invasion of privacy of American citizens whose private and personal telegrams were intercepted as a result of their being on the NSA watch list from 1967 to 1973.

It resulted in companies betraying the trust of their paying customers who had a right to expect that the messages would be handled confidentially. It was undertaken without the companies first ascertaining its legality. It was not disclosed to the Congress until this year. Finally, it continued without interruption for nearly 30 years, even though apparently no express approval of the project was obtained from any President, Attorney General, or Secretary of Defense after 1949.

The CHAIRMAN. Would any other Senator like to comment?

Then I might just add to what Senator Hart said, that after 1947, the program changed without notice to the companies. It changed in ways that really placed the responsibility on the Government to notify the companies of the change in character of the program, and this apparently was not done.

I do not think that there is any purpose to be served debating the issue any further, but I would like to say that the lack of any statutory

base for NSA, establishing its proper limits, is one of the problems, and there came a time when even the NSA had doubts about the legality of this program, and also whether it extended beyond the scope of that Agency's own purpose and authority. For that reason, the Agency itself finally terminated the program, but such programs can be re-instituted after investigations of this kind. I think it is clear that laws are needed, a basic law for the NSA, just as we have a basic law for the CIA.

Senator TOWER. Mr. Chairman?

The CHAIRMAN. Senator Tower.

Senator TOWER. I would simply like to say that my remarks were not intended to endorse or condone the activity in question because I do not endorse or condone it. But I strongly object to the disclosure because I think it serves no useful purpose. The Agency has been very cooperative with the committee in making disclosures to the committee to enable us to pursue our investigation effectively. I think that disclosure serves no useful purpose, and I think that when we get to the question of public disclosure, that if we err in terms of withholding information or publishing information, that we should err on the side of safety and I think that we have not done that in this instance. I think that at this point, should this be considered a precedent, and should we pursue this pattern of disclosure in the future, then this committee will have effectively crippled the intelligence-gathering capability of the United States of America.

Senator GOLDWATER. Mr. Chairman.

The CHAIRMAN. Senator Goldwater.

Senator GOLDWATER. I guess a lot of us are guilty of operations like this because many of us censored letters during World War II, reading those letters. So I think I would have to join the guilty as you would have to, also.

The CHAIRMAN. I think that we should recognize the distinction between war and peace. It poses the question whether this country in peacetime wants to live always under the customs of war. This was a peacetime operation.

Senator MATHIAS. Mr. Chairman?

Senator TOWER. Mr. Chairman.

The CHAIRMAN. In any case—

Senator MATHIAS. Mr. Chairman.

The CHAIRMAN. Senator Mathias.

Senator MATHIAS. Senator Goldwater indicted those who had that long and tedious duty of reading letters during World War II. I certainly read at least my share, and I expect a little more than my share. I would say it was perhaps the most boring duty I had in the entire period of service in the U.S. Navy, but I would have to plead not guilty because I think the circumstances were very different. One of the different circumstances is the fact that what was done there was done in accordance with the law. The law provided—in fact, the law compelled us to read those letters and to make the appropriate changes that were required, and it is the law that I think is important here. I think that the law does not extend to the activities of the NSA. The law must be made to extend to the NSA. That certainly is going to be one of the cardinal recommendations of this committee at the conclusion of its work.

The CHAIRMAN. Thank you.

Senator TOWER. Mr. Chairman.

The CHAIRMAN. Senator Tower.

Senator Tower. I think to make fine distinctions on a matter of war and peace ignores the fact that we are confronted in this world by a very powerful adversary that would not hesitate to resort to military means to achieve its political objectives. A powerful adversary that itself, through its clandestine activities and overt activities, generates military activity all over the world to accomplish political ends, thereby jeopardizing the peace and security of everybody in this world who aspires to self-determination and wants to have some reasonable hope of the realization of that aspiration.

So I think that we cannot draw this in strict terms of war and peace, in terms of whether or not the United States is actually at war. We are in effect in a war of sorts. That is a war of the preservation of the climate in this world where national integrity will be respected.

The CHAIRMAN. Thank you, Senator Tower.

I would only make a final point. Since we are trying to preserve a free society we do not want to emulate the methods of the Russians in the name of defense. The actions we do take of a proper security nature and proper intelligence nature ought to be within the confines of the law. There are ways that we can write the law and preserve freedom in this country and still maintain our security against the Russian threat or any other foreign threat. And 200 years of American history testifies to this.

Senator TOWER. May I say I do not condemn the investigation, nor do I endorse what was done. It was wrong and without the law, but what I object to is the disclosure because I think it serves no useful purpose and is helpful to the adversary.

The CHAIRMAN. Thank you, Senator.

I would like now to invite the Attorney General of the United States to come in.

Mr. Attorney General, if you would please be seated at the witness stand.

Before I introduce the Attorney General, Senator Schweiker has a comment.

Senator SCHWEIKER. The debate that we just had points out very clearly the lack of law in a very critical area. I hope the debate will highlight the fact that laws are needed and that there is honest room to differ among members of this committee. I think that is our first and most significant aspect of the discussion. I happen to decide this issue on the basis that the public's right to know outweighs any danger that might exist to the Government.

In this case I think it was a matter more of embarrassment to the Government than a matter of damaging security. But I think it was because we did not have law, and because the area was in a vacuum, that we got into this kind of debate. I believe because it was the kind of Government snooping that I personally could not condone, that the committee and my standard in this case was that silence is consent. I thought that the committee and I had a right to speak out on this matter because I believe to be silent would be to give consent. That is why I voted consistently to release this. Thank you.

The CHAIRMAN. Thank you, Senator Schweiker. And I would hope that corporations in the future may find it possible because of the ways the laws are written to cooperate with the Government in the public interest. I think we all agree on that.

The Attorney General of the United States has been invited to appear before the select committee today to discuss the fourth amendment of the Constitution and its application to 20th century problems of intelligence and surveillance. In the case of the NSA, which is of particular concern to us today, the rapid development of technology in the area of electronic surveillance has seriously aggravated present ambiguities in the law. The broad sweep of communications interception by NSA takes us far beyond previous fourth amendment controversies where particular individuals and specific telephone lines were the target.

How can we control this sophisticated technology allowing NSA to perform its legitimate foreign intelligence task without also allowing it to invade the privacy of American citizens by sweeping in messages unrelated to the interests of national security? What are we to do about communications that fall outside the realm of traditional intelligence concerns, such as the vague category of economic or business intelligence? Are we to allow communications to or from U.S. citizens regarding economic matters to be intercepted, analyzed and disseminated by NSA? In an era of economic crisis are the international phone calls and cables of American businessmen fair game for government computers? If so, should warrants or some other special procedure be required? These are matters of the most serious concern. The central question is: How should we balance the right to privacy against the need for national security?

Mr. Attorney General, your appearance here marks an important step on the road to more effective controls in these areas. As you know, in addition to practices of the NSA, the committee has also received considerable testimony on the subject of break-ins and mail openings and other such factors. We are hopeful that we can explore all of these subjects with you today. We value your views on the basic principles at stake and we look forward to working together with you to develop legislative recommendations which will help solve these dilemmas.

I understand that you have prepared a statement and have given very careful thought to this question, and I recognize that the statement is somewhat lengthy because of the subject, that can hardly be treated in a truncated fashion. So I invite you now to read your statement.

Attorney General LEVI. Thank you, Mr. Chairman. I have a lengthy statement that I have shortened somewhat, hoping to help the committee in that respect—

Senator MATHIAS. Mr. Chairman, I am wondering whether the Attorney General would yield for just a moment, so that I could request that his statement in its entirety be included as part of the record because I believe that it will be a very valuable part of this record. We need the benefit of all of it, although he may be inclined to somewhat shorten it in his oral presentation.

The CHAIRMAN. I fully agree, and without objection the original statement in its entirety will be included in the record.

[The prepared statement of Attorney General Levi in full follows:]

PREPARED STATEMENT OF HON. EDWARD H. LEVI, ATTORNEY GENERAL OF THE  
UNITED STATES

I am here today in response to a request from the Committee to discuss the relationship between electronic surveillance and the Fourth Amendment of the Constitution. If I remember correctly, the original request was that I place before the Committee the philosophical or jurisprudential framework relevant to this relationship which lawyers, those with executive responsibilities or discretion, and lawmakers, viewing this complex field, ought to keep in mind. If this sounds vague and general and perhaps useless, I can only ask for indulgence. My first concern when I received the request was that any remarks I might be able to make would be so general as not to be helpful to the Committee. But I want to be as helpful to the Committee as I can be.

The area with which the Committee is concerned is a most important one. In my view, the development of the law in this area has not been satisfactory, although there are reasons why the law has developed as it has. Improvement of the law, which in part means its clarification, will not be easy. Yet it is a most important venture. In a talk before the American Bar Association last August, I discussed some of the aspects of the legal framework. Speaking for the Department of Justice, I concluded this portion of the talk with the observation and commitment that "we have very much in mind the necessity to determine what procedures through legislation, court action or executive processes will best serve the national interest, including, of course, the protection of constitutional rights."

I begin then with an apology for the general nature of my remarks. This will be due in part to the nature of the law itself in this area. But I should state at the outset there are other reasons as well. In any area, and possibly in this one more than most, legal principles gain meaning through an interaction with the facts. Thus, the factual situations to be imagined are of enormous significance.

As this Committee well knows, some of the factual situations to be imagined in this area are not only of a sensitive nature but also of a changing nature. Therefore, I am limited in what I can say about them, not only because they are sensitive, but also because a lawyer's imagination about future scientific developments carries its own warnings of ignorance. This is a point worth making when one tries to develop appropriate safeguards for the future.

There is an additional professional restriction upon me which I am sure the Committee will appreciate. The Department of Justice has under active criminal investigation various activities which may or may not have been illegal. In addition, the Department through its own attorneys, or private attorneys specially hired, is representing present or former government employees in civil suits which have been brought against them for activities in the course of official conduct. These circumstances naturally impose some limitation upon what it is appropriate for me to say in this forum. I ought not give specific conclusory opinions as to matters under criminal investigation or in litigation. I can only hope that what I have to say may nevertheless be of some value to the Committee in its search for constructive solutions.

I do realize there has to be some factual base, however unfocused it may at times have to be, to give this discussion meaning. Therefore, as a beginning, I propose to recount something of the history of the Department's position and practice with respect to the use of electronic surveillance, both for telephone wiretapping and for trespassory placement of microphones.

As I read the history, going back to 1931 and undoubtedly prior to that time, except for an interlude between 1928 and 1931, and for two months in 1940, the policy of the Department of Justice has been that electronic surveillance could be employed without a warrant in certain circumstances.

In 1928 the Supreme Court in *Olmstead v. United States* held that wiretapping was not within the coverage of the Fourth Amendment. Attorney General Sargent had issued an order earlier in the same year prohibiting what was then known as the Bureau of Investigation from engaging in any telephone wiretapping for any reason. Soon after the order was issued, the Prohibition Unit was transferred to the Department as a new bureau. Because of the nature of its work and the fact that the Unit had previously engaged in telephone wiretapping, in January 1931, Attorney General William D. Mitchell directed that a study be made to determine whether telephone wiretapping should be permitted and, if so, under what circumstances. The Attorney General determined that in the meantime the bureaus within the Department could engage in

telephone wiretapping upon the personal approval of the bureau chief after consultation with the Assistant Attorney General in charge of the case. The policy during this period was to allow wiretapping only with respect to the telephones of syndicated bootleggers, where the agent had probable cause to believe the telephone was being used for liquor operations. The bureaus were instructed not to tap telephones of public officials and other persons not directly engaged in the liquor business. In December 1931, Attorney General William Mitchell expanded the previous authority to include "exceptional cases where the crimes are substantial and serious, and the necessity is great and [the bureau chief and the Assistant Attorney General] are satisfied that the persons whose wires are to be tapped are of the criminal type."

During the rest of the thirties it appears that the Department's policy concerning telephone wiretapping generally conformed to the guidelines adopted by Attorney General William Mitchell. Telephone wiretapping was limited to cases involving the safety of the victim (as in kidnappings), location and apprehension of "desperate" criminals, and other cases considered to be of major law enforcement importance, such as espionage and sabotage.

In December 1937, however, in the first *Nardone* case the United States Supreme Court reversed the Court of Appeals for the Second Circuit, and applied Section 605 of the Federal Communications Act of 1934 to law enforcement officers; thus rejecting the Department's argument that it did not so apply. Although the Court read the Act to cover only wire interceptions where there had also been disclosure in court or to the public, the decision undoubtedly had its impact upon the Department's estimation of the value of telephone wiretapping as an investigative technique. In the second *Nardone* case in December 1939, the Act was read to bar the use in court not only of the overheard evidence, but also of the fruits of that evidence. Possibly for this reason, and also because of public concern over telephone wiretapping, on March 15, 1940, Attorney General Robert Jackson imposed a total ban on its use by the Department. This ban lasted about two months.

On May 21, 1940, President Franklin Roosevelt issued a memorandum to the Attorney General stating his view that electronic surveillance would be proper under the Constitution where "grave matters involving defense of the nation" were involved. The President authorized and directed the Attorney General "to secure information by listening devices [directed at] the conversation or other communications of persons suspected of subversive activities against the Government of the United States, including suspected spies." The Attorney General was requested "to limit these investigations so conducted to a minimum and to limit them insofar as possible as to aliens." Although the President's memorandum did not use the term "trespassory microphone surveillance," the language was sufficiently broad to include that practice, and the Department construed it as an authorization to conduct trespassory microphone surveillances as well as telephone wiretapping in national security cases. The authority for the President's action was later confirmed by an opinion by Assistant Solicitor General Charles Fahy who advised the Attorney General that electronic surveillance could be conducted where matters affected the security of the nation.

On July 17, 1946, Attorney General Tom C. Clark sent President Truman a letter reminding him that President Roosevelt had authorized and directed Attorney General Jackson to approve "listening devices [directed at] the conversation of other communications of persons suspected of subversive activities against the Government of the United States, including suspected spies" and that the directive had been followed by Attorneys General Robert Jackson and Francis Biddle. Attorney General Clark recommended that the directive "be continued in force" in view of the "increase in subversive activities" and "a very substantial increase in crime." He stated that it was imperative to use such techniques "in cases vitally affecting the domestic security, or where human life is in jeopardy" and that Department files indicated that his two most recent predecessors as Attorney General would concur in this view. President Truman signed his concurrence on the Attorney General's letter.

According to the Department's records, the annual total of telephone wiretaps and microphones installed by the Bureau between 1940 through 1951 was as follows:

Telephone wiretaps :		Microphones :	
1940	6	1940	6
1941	67	1941	25
1942	304	1942	88
1943	475	1943	193
1944	517	1944	198
1945	519	1945	186
1946	364	1946	84
1947	374	1947	81
1948	416	1948	67
1949	471	1949	75
1950	270	1950	61
1951	285	1951	75

It should be understood that these figures, as is the case for the figures I have given before, are cumulative for each year and also duplicative to some extent, since a telephone wiretap or microphone which was installed, then discontinued, but later reinstated would be counted as a new action upon reinstatement.

In 1952, there were 285 telephone wiretaps, 300 in 1953, and 322 in 1954. Between February 1952 and May 1954, the Department's position was not to authorize trespassory microphone surveillance. This was the position taken by Attorney General McGrath, who informed the FBI that he would not approve the installation of trespassory microphone surveillance because of his concern over a possible violation of the Fourth Amendment. FBI records indicate there were 63 microphones installed in 1952, there were 52 installed in 1953, and there were 99 installed in 1954. The policy against Attorney General approval, at least in general, of trespassory microphone surveillance was reversed by Attorney General Herbert Brownell on May 20, 1954, in a memorandum to Director Hoover instructing him that the Bureau was authorized to conduct trespassory microphone surveillances. The Attorney General stated that "considerations of internal security and the national safety are paramount and, therefore, may compel the unrestricted use of this technique in the national interest."

A memorandum from Director Hoover to the Deputy Attorney General on May 4, 1961, described the Bureau's practice since 1954 as follows: "[I]n the internal security field, we are utilizing microphone surveillances on a restricted basis even though trespass is necessary to assist in uncovering the activities of Soviet intelligence agents and Communist Party leaders. In the interests of national safety, microphone surveillances are also utilized on a restricted basis, even though trespass is necessary, in uncovering major criminal activities. We are using such coverage in connection with our investigations of the clandestine activities of top hoodlums and organized crime. From an intelligence standpoint, this investigative technique has produced results unobtainable through other means. The information so obtained is treated in the same manner as information obtained from wiretaps, that is, not from the standpoint of evidentiary value but for intelligence purposes."

The number of telephone wiretaps and microphones from 1955 through 1964 was as follows:

Telephone wiretaps :		Microphones :	
1955	214	1955	102
1956	164	1956	71
1957	173	1957	73
1958	166	1958	70
1959	120	1959	75
1960	115	1960	74
1961	140	1961	85
1962	198	1962	100
1963	244	1963	83
1964	260	1964	106

It appears that there was a change in the authorization procedure for microphone surveillance in 1965. A memorandum of March 30, 1965, from Director Hoover to the Attorney General states that "[i]n line with your suggestion this morning, I have already set up the procedure similar to requesting of authority for phone taps to be utilized in requesting authority for the placement of microphones."

President Johnson announced a policy for federal agencies in June 1965 which required that the interception of telephone conversations without the consent of one of the parties be limited to investigations relating to national security and

that the consent of the Attorney General be obtained in each instance. The memorandum went on to state that use of mechanical or electronic devices to overhear conversations not communicated by wire is an even more difficult problem "which raises substantial and unresolved questions of Constitutional interpretation." The memorandum instructed each agency conducting such an investigation to consult with the Attorney General to ascertain whether the agency's practices were fully in accord with the law. Subsequently, in September 1965, the Director of the FBI wrote the Attorney General and referred to the "present atmosphere, brought about by the unrestrained and injudicious use of special investigative techniques by other agencies and departments, resulting in Congressional and public alarm and opposition to any activity which could in any way be termed an invasion of privacy." "As a consequence," the Director wrote, "we have discontinued completely the use of microphones." The Attorney General responded in part as follows: "The use of wiretaps and microphones involving trespass present more difficult problems because of the inadmissibility of any evidence obtained in court cases and because of current judicial and public attitude regarding their use. It is my understanding that such devices will not be used without my authorization, although in emergency circumstances they may be used subject to my later ratification. At this time I believe it desirable that all such techniques be confined to the gathering of intelligence in national security matters, and I will continue to approve all such requests in the future as I have in the past. I see no need to curtail any such activities in the national security field."

The policy of the Department was stated publicly by the Solicitor General in a supplemental brief in the Supreme Court in *Black v. United States* in 1966. Speaking of the general delegation of authority by Attorneys General to the Director of the Bureau, the Solicitor General stated in his brief:

"An exception to the general delegation of authority has been prescribed, since 1940, for the interception of wire communications, which (in addition to being limited to matters involving national security or danger to human life) has required the specific authorization of the Attorney General in each instance. No similar procedure existed until 1965 with respect to the use of devices such as those involved in the instant case, although records of oral and written communications within the Department of Justice reflect concern by Attorneys General and the Director of the Federal Bureau of Investigation that the use of listening devices by agents of the government should be confined to a strictly limited category of situations. Under Departmental practice in effect for a period of years prior to 1965, and continuing until 1965, the Director of the Federal Bureau of Investigation was given authority to approve the installation of devices such as that in question for intelligence (and not evidentiary) purposes when required in the interests of internal security or national safety, including organized crime, kidnappings and matters wherein human life might be at stake...."

Present Departmental practice, adopted in July 1965 in conformity with the policies declared by the President on June 30, 1965, for the entire federal establishment, prohibits the use of such listening devices (as well as the interception of telephone and other wire communications) in all instances other than those involving the collection of intelligence affecting the national security. The specific authorization of the Attorney General must be obtained in each instance when this exception is invoked."

The Solicitor General made a similar statement in another brief filed that same term (*Schipani v. U.S.*) again emphasizing that the data would not be made available for prosecutorial purposes, and that the specific authorization of the Attorney General must be obtained in each instance when the national security is sought to be invoked. The number of telephone wiretaps and microphones installed since 1965 are as follows:

Telephone wiretaps:		Microphones:	
1965	233	1965	67
1966	174	1966	10
1967	113	1967	0
1968	82	1968	9
1969	123	1969	14
1970	102	1970	19
1971	101	1971	16
1972	108	1972	32
1973	123	1973	40
1974	190	1974	42

Comparable figures for the year 1975 up to October 29 are:

Telephone wiretaps: 121  
Microphones: 24

In 1968 Congress passed the Omnibus Crime Control and Safe Streets Act. Title III of the Act set up a detailed procedure for the interception of wire or oral communications. The procedure requires the issuance of a judicial warrant, prescribes the information to be set forth in the petition to the judge so that, among other things, he may find probable cause that a crime has been or is about to be committed. It requires notification to the parties subject to the intended surveillance within a period not more than ninety days after the application for an order of approval has been denied or after the termination of the period of the order or the period of the extension of the order. Upon a showing of good cause the judge may postpone the notification. The Act contains a saving clause to the effect that it does not limit the constitutional power of the President to take such measures as he deems necessary to protect the nation against actual or potential attack or other hostile acts of a foreign power, to obtain foreign intelligence information deemed essential to the security of the United States, or to protect national security information against foreign intelligence activities. Then in a separate sentence the proviso goes on to say, "Nor shall anything contained in this chapter be deemed to limit the constitutional power of the President to take such measures as he deems necessary to protect the United States against the overthrow of the government by force or other unlawful means, or against any other clear and present danger to the structure or existence of the government."

The Act specifies the conditions under which information obtained through a presidentially authorized interception might be received into evidence. In speaking of this saving clause, Justice Powell in the *Keith* case in 1972 wrote: "Congress simply left presidential powers where it found them." In the *Keith* case the Supreme Court held that in the field of internal security, if there was no foreign involvement, a judicial warrant was required for the Fourth Amendment. Fifteen months after the *Keith* case Attorney General Richardson, in a letter to Senator Fulbright which was publicly released by the Department, stated: "In general, before I approve any new application for surveillance without a warrant, I must be convinced that it is necessary (1) to protect the nation against actual or potential attack or other hostile acts of a foreign power; (2) to obtain foreign intelligence information deemed essential to the security of the United States; or (3) to protect national security information against foreign intelligence activities."

I have read the debates and the reports of the Senate Judiciary Committee with respect to Title III and particularly the proviso. It may be relevant to point out that Senator Philip Hart questioned and opposed the form of the proviso reserving presidential power. But I believe it is fair to say that his concern was primarily, perhaps exclusively, with the language which dealt with presidential power to take such measures as the President deemed necessary to protect the United States "against any other clear and present danger to the structure or existence of the Government."

I now come to the Department of Justice's present position on electronic surveillance conducted without a warrant. Under the standards and procedures established by the President, the personal approval of the Attorney General is required before any non-consensual electronic surveillance may be instituted within the United States without a judicial warrant. All requests for surveillance must be made in writing by the Director of the Federal Bureau of Investigation and must set forth the relevant circumstances that justify the proposed surveillance. Both the agency and the Presidential appointee initiating the request must be identified. These requests come to the Attorney General after they have gone through review procedures within the Federal Bureau of Investigation. At my request, they are then reviewed in the Criminal Division of the Department. Before they come to the Attorney General, they are then examined by a special review group which I have established within the Office of the Attorney General. Each request, before authorization or denial, receives my personal attention. Requests are only authorized when the requested electronic surveillance is necessary to protect the nation against actual or potential attack or other hostile acts of a foreign power; to obtain foreign intelligence deemed essential to the security of the nation; to protect national security information against foreign intelligence activities; or to obtain information certified as

necessary for the conduct of foreign affairs matters important to the national security of the United States. In addition the subject of the electronic surveillance must be consciously assisting a foreign power or foreign-based political group, and there must be assurance that the minimum physical intrusion necessary to obtain the information sought will be used. As these criteria will show and as I will indicate at greater length later in discussing current guidelines the Department of Justice follows, our concern is with respect to foreign powers or their agents. In a public statement made last July 9th, speaking of the warrantless surveillances then authorized by the Department, I said "it can be said that there are no outstanding instances of warrantless wiretaps or electronic surveillance directed against American citizens and none will be authorized by me except in cases where the target of surveillance is an agent or collaborator of a foreign power." This statement accurately reflects the situation today as well.

Having described in this fashion something of the history and conduct of the Department of Justice with respect to telephone wiretaps and microphone installations, I should like to remind the Committee of a point with which I began, namely, that the factual situations to be imagined for a discussion such as this are not only of a sensitive but a changing nature. I do not have much to say about this except to recall some of the language used by General Allen in his testimony before this Committee. The techniques of the NSA, he said, are of the most sensitive and fragile character. He described as the responsibility of the NSA the interception of international communication signals sent through the air. He said there had been a watch list, which among many other names, contained the names of U.S. citizens. Senator Tower spoke of an awesome technology—a huge vacuum cleaner of communications—which had the potential for abuses. General Allen pointed out that "The United States, as part of its effort to produce foreign intelligence, has intercepted foreign communications, analyzed, and in some cases decoded, these communications to produce such foreign intelligence since the Revolutionary War." He said the mission of NSA is directed to foreign intelligence obtained from foreign electrical communications and also from other foreign signals such as radar. Signals are intercepted by many techniques and processed, sorted and analyzed by procedures which reject inappropriate or unnecessary signals. He mentioned that the interception of communications, however it may occur, is conducted in such a manner as to minimize the unwanted messages. Nevertheless, according to his statement, many unwanted communications are potentially selected for further processing. He testified that subsequent processing, sorting and selection for analysis are conducted in accordance with strict procedures to insure immediate and, wherever possible, automatic rejection of inappropriate messages. The analysis and reporting is accomplished only for those messages which meet specific conditions and requirements for foreign intelligence. The use of lists of words, including individual names, subjects, locations, et cetera, has long been one of the methods used to sort out information of foreign intelligence value from that which is not of interest.

General Allen mentioned a very interesting statute, 18 USC 952, to which I should like to call your particular attention. The statute makes it a crime for any one who by virtue of his employment by the United States obtains any official diplomatic code and willfully publishes or furnishes to another without authorization any such code or any other matter which was obtained while in the process of transmission between any foreign government and its diplomatic mission in the United States. I call this to your attention because a certain indirection is characteristic of the development of law, whether by statute or not, in this area.

The Committee will at once recognize that I have not attempted to summarize General Allen's testimony, but rather to recall it so that this extended dimension of the variety of fact situations which we have to think about as we explore the coverage and direction of the Fourth Amendment is at least suggested.

Having attempted to provide something of a factual base for our discussion, I turn now to the Fourth Amendment. Let me say at once, however, that while the Fourth Amendment can be a most important guide to values and procedures, it does not mandate automatic solutions.

The history of the Fourth Amendment is very much the history of the American Revolution and this nation's quest for independence. The Amendment is the legacy of our early years and reflects values most cherished by the Founders. In a direct sense, it was a reaction to the general warrants and writs of assistance employed by the officers of the British Crown to rummage and ransack colonists' homes as a means to enforce antismuggling and customs laws. General

search warrants had been used for centuries in England against those accused of seditious libel and other offenses. These warrants, sometimes judicial, sometimes not, often general as to persons to be arrested, places to be searched, and things to be seized, were finally condemned by Lord Camden in 1765 in *Entick v. Carrington*, a decision later celebrated by the Supreme Court in *Boyd v. United States* as a "landmark of English liberty . . . one of the permanent monuments of the British Constitution." The case involved a general warrant, issued by Lord Halifax as Secretary of State, authorizing messengers to search for John Entick and to seize his private papers and books. Entick had written publications criticizing the Crown and was a supporter of John Wilkes, the famous author and editor of the *North Briton* whose own publications had prompted wholesale arrests, searches, and seizures. Entick sued for trespass and obtained a jury verdict in his favor. In upholding the verdict, Lord Camden observed that if the government's power to break into and search homes were accepted, "the secret cabinets and bureaus of every subject in this kingdom would be thrown open to the search and inspection of a messenger, whenever the secretary of state shall see fit to charge, or even to suspect, a person to be the author, printer, or publisher of a seditious libel."

The practice of the general warrants, however, continued to be known in the colonies. The writ of assistance, an even more arbitrary and oppressive instrument than the general warrant, was also widely used by revenue officers to detect smuggled goods. Unlike a general warrant, the writ of assistance was virtually unlimited in duration and did not have to be returned to the court upon its execution. It broadly authorized indiscriminate searches and seizures against any person suspected by a customs officer of possessing prohibited or uncustomed goods. The writs, sometimes judicial, sometimes not, were usually issued by colonial judges and vested Crown officers with unreviewed and unbounded discretion to break into homes, rifle drawers, and seize private papers. All officers and subjects of the Crown were further commanded to assist in the writ's execution. In 1761 James Otis eloquently denounced the writs as "the worst instrument of arbitrary power, the most destructive of English liberty, and the fundamental principles of law, that ever was found in an English law book," since they put "the liberty of every man in the hands of every petty officer." Otis' fiery oration later prompted John Adams to reflect that "then and there was the first scene of the first act of opposition to the arbitrary claims of Great Britain. Then and there the child Independence was born."

The words of the Fourth Amendment are mostly the product of James Madison. His original version appeared to be directed solely at the issuance of improper warrants.<sup>1</sup> Revisions accomplished under circumstances that are still unclear transformed the Amendment into two separate clauses. The change has influenced our understanding of the nature of the rights it protects. As embodied in our Constitution, the Amendment reads: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

Our understanding of the purposes underlying the Fourth Amendment has been an evolving one. It has been shaped by subsequent historical events, by the changing conditions of our modern technological society, and by the development of our own traditions, customs, and values. From the beginning, of course, there has been agreement that the Amendment protects against practices such as those of the Crown officers under the notorious general warrants and writs of assistance. Above all, the Amendment safeguards the people from unlimited, undue infringement by the government on the security of persons and their property.

But our perceptions of the language and spirit of the Amendment have gone beyond the historical wrongs the Amendment was intended to prevent. The Supreme Court has served as the primary explicator of these evolving perceptions and has sought to articulate the values the Amendment incorporates. I believe it is useful in our present endeavor to identify some of these perceived values.

---

<sup>1</sup> Madison's proposal read as follows: "The rights of the people to be secured in their persons, their houses, their papers, and their other property, from all unreasonable searches and seizures, shall not be violated by warrants issued without probable cause, supported by oath or affirmation, or not particularly describing the places to be searched, or the persons or things to be seized."

First, broadly considered, the Amendment speaks to the autonomy of the individual against society. It seeks to accord to each individual, albeit imperfectly, a measure of the confidentiality essential to the attainment of human dignity. It is a shield against indiscriminate exposure of an individual's private affairs to the world—an exposure which can destroy, since it places in jeopardy the spontaneity of thought and action on which so much depends. As Justice Brandeis observed in his dissent in the *Olmstead* case, in the Fourth Amendment the Founders "conferred, as against the Government, the right to be let alone—the most comprehensive of rights and the right most valued by civilized men." Judge Jerome Frank made the same point in a dissent in a case in which a paid informer with a concealed microphone broadcast an intercepted conversation to a narcotics agent. Judge Frank wrote in *United States v. On Lee* that "[a] sane, decent, civilized society must provide some such oasis, some shelter from public scrutiny, some insulated enclosure some enclave, some inviolate place which is a man's castle." The Amendment does not protect absolutely the privacy of an individual. The need for privacy, and the law's response to that need, go beyond the Amendment. But the recognition of the value of individual autonomy remains close to the Amendment's core.

A parallel value has been the Amendment's special concern with intrusions when the purpose is to obtain evidence to incriminate the victim of the search. As the Supreme Court observed in *Boyd*, which involved an attempt to compel the production of an individual's private papers, at some point the Fourth Amendment's prohibition against unreasonable searches and seizures and the Fifth Amendment's prohibition against compulsory self-incrimination "run almost into each other." The intrusion on an individual's privacy has long been thought to be especially grave when the search is based on a desire to discover incriminating evidence.<sup>2</sup> The desire to incriminate may be seen as only an aggravating circumstance of the search, but it has at times proven to be a decisive factor in determining its legality. Indeed, in *Boyd* the Court declared broadly that "compelling the production of [a person's] private books and papers, to convict him of crime, or to forfeit his property, is contrary to the principles of a free government."

The incriminating evidence point goes to the integrity of the criminal justice system. It does not necessarily settle the issue whether the overhearing can properly take place. It goes to the use and purpose of the information overheard.

An additional concern of the Amendment has been the protection of freedom of thought, speech, and religion. The general warrants were used in England as a powerful instrument to suppress what was regarded as seditious libel or non-conformity. Wilkes was imprisoned in the Tower and all his private papers seized under such a warrant for his criticism of the King. As Justice Frankfurter inquired, dissenting in *Harris v. United States*, a case that concerned the permissible scope of searches incident to arrest, "How can there be freedom of thought or freedom of speech or freedom of religion, if the police can, without warrant, search your house and mine from garret to cellar . . .?" So Justice Powell stated in *Keith* that "Fourth Amendment protections become the more necessary when the targets of official surveillance may be those suspected of unorthodoxy in their political beliefs."

Another concern embodied in the Amendment may be found in its second clause dealing with the warrant requirement, even though the Fourth Amendment does not always require a warrant. The fear is that the law enforcement officer, if unchecked, may misuse his powers to harass those who hold unpopular or simply different views and to intrude capriciously upon the privacy of individuals. It is the recognition of the possibility for abuse, inherent whenever executive discretion is uncontrolled, that gives rise to the requirement of a warrant. That requirement constitutes an assurance that the judgment of a neutral and detached magistrate will come to bear before the intrusion is made and that the decision whether the privacy of the individual must yield to a greater need of society will not be left to the executive alone.

---

<sup>2</sup>The concern with self-incrimination is reflected in the test of standing to invoke the exclusionary rule. As the Court stated in *United States v. Calandra*: "Thus, standing to invoke the exclusionary rule [under the Fourth Amendment] has been confined to situations where the Government seeks to use such evidence to incriminate the victim of the unlawful search. . . . This standing rule is premised on a recognition that the need for deterrence, and hence the rationale for excluding the evidence are strongest where the Government's unlawful conduct would result in imposition of a criminal sanction on the victim of the search."

A final value reflected in the Fourth Amendment is revealed in its opening words: "The right of the people." Who are "the people" to whom the Amendment refers? The Constitution begins with the phrase, "We the People of the United States." That phrase has the character of words of art, denoting the power from which the Constitution comes. It does suggest a special concern for the American citizen and for those who share the responsibilities of citizens. The Fourth Amendment guards the right of "the people" and it can be urged that it was not meant to apply to foreign nations, their agents and collaborators. Its application may at least take account of that difference.

The values outlined above have been embodied in the Amendment from the beginning. But the importance accorded a particular value has varied during the course of our history. Some have been thought more important or more threatened than others at times. When several of the values coalesce, the need for protection has been regarded as greatest. When only one is involved, that need has been regarded as lessened. Moreover, the scope of the Amendment itself has been altered over time, expanding or contracting in the fact of changing circumstances and needs. As with the evolution of other constitutional provisions, this development has been case in definitional terms. Words have been read by different Justices and different Courts to mean different things. The words of the Amendment have not changed; we, as a people, and the world which envelops us, have changed.

An important example is what the Amendment seeks to guard as "secure." The wording of the Fourth Amendment suggests a concern with tangible property. By its terms, the Amendment protects the right of the people to be secure in their "persons, houses, papers and effects." The emphasis appears to be on the material possessions of a person, rather than on his privacy generally. The Court came to that conclusion in 1928 in the *Olmstead* case, holding that the interception of telephone messages, if accomplished without a physical trespass, was outside the scope of the Fourth Amendment. Chief Justice Taft, writing for the Court, reasoned that wiretapping did not involve a search or seizure; the Amendment protected only tangible material "effects" and not intangibles such as oral conversations. A thread of the same idea can be found in *Entick*, where Lord Camden said: "The great end for which men entered into society was to secure their property." But, while the removal and carrying off of papers was a trespass of the most aggravated sort, inspection alone was not: "the eye," Lord Camden said, "cannot by the law of England be guilty of a trespass."

The movement of the law since *Olmstead* has been steadily from protection of property to protection of privacy. In the *Goldman* case in 1942 the Court held that the use of a detectaphone placed against the wall of a room to overhear oral conversations in an adjoining office was not unlawful because no physical trespass was involved. The opinion's unstated assumption, however, appeared to be that a private oral conversation could be among the protected "effects" within the meaning of the Fourth Amendment. The *Silberman* case later eroded *Olmstead* substantially by holding that the Amendment was violated by the interception of an oral conversation through the use of a spike mike driven into a party wall, penetrating the heating duct of the adjacent home. The Court stated that the question whether a trespass had occurred as a technical matter of property law was not controlling; the existence of an actual intrusion was sufficient.

The Court finally reached the opposite emphasis from its previous stress on property in 1967 in *Katz v. United States*. The Court declared that the Fourth Amendment "protects people, not places," against unreasonable searches and seizures; that oral conversations, although intangible, were entitled to be secure against the uninvited ear of a government officer, and that the interception of a telephone conversation, even if accomplished without a trespass, violated the privacy on which petitioner justifiably relied while using a telephone booth. Justice Harlan, in a concurring opinion, explained that to have a constitutionally protected right of privacy under *Katz* it was necessary that a person, first, "have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'"

At first glance, *Katz* might be taken as a statement that the Fourth Amendment now protects all reasonable expectations of privacy—that the boundaries of the right of privacy are coterminous with those of the Fourth Amendment. But that assumption would be misleading. To begin with the Amendment still protects some interests that have very little if any thing to do with privacy. Thus, the police may not, without warrant, seize an automobile parked on the owner's

driveway even though they have reason to believe that the automobile was used in committing a crime. The interest protected by the Fourth Amendment in such a case is probably better defined in terms of property than privacy. Moreover, the *Katz* opinion itself cautioned that "the Fourth Amendment cannot be translated into a general constitutional 'right to privacy.'" Some privacy interests are protected by remaining Constitutional guarantees. Others are protected by federal statute, by the states, or not at all.

The point is twofold. First, under the Court's decisions, the Fourth Amendment does not protect every expectation of privacy, no matter how reasonable or actual that expectation may be. It does not protect, for example, against false friends' betrayals to the police of even the most private confidences. Second, the "reasonable expectation of privacy" standard, often said to be the test of *Katz*, is itself a conclusion. It represents a judgment that certain behavior should as a matter of law be protected against unrestrained governmental intrusion. That judgment, to be sure, rests in part on an assessment of the reasonableness of the expectation, that is, on an objective, factual estimation of a risk of intrusion under given circumstances, joined with an actual expectation of privacy by the person involved in a particular case. But it is plainly more than that, since it is also intermingled with a judgment as to how important it is to society that an expectation should be confirmed—a judgment based on a perception of our customs, traditions, and values as a free people.

The *Katz* decision itself illustrates the point. Was it really a "reasonable expectation" at the time of *Katz* for a person to believe that his telephone conversation in a public phone booth was private and not susceptible to interception by a microphone on the booth's outer wall? Almost forty years earlier in *Olmstead* the Court held that such nontrespassory interceptions were permissible. *Goldman* reaffirmed that holding. So how could *Katz* reasonably expect the contrary? The answer, I think, is that the Court's decision in *Katz* turned ultimately on an assessment of the effect of permitting such unrestrained intrusions on the individual in his private and social life. The judgment was that a license for unlimited governmental intrusions upon every telephone would pose too great a danger to the spontaneity of human thought and behavior. Justice Harlan put the point this way in *United States v. White*:

"The analysis must, in my view, transcend the search for subjective expectations or legal attribution of assumptions of risk. Our expectations, and the risks we assume, are in large part reflections of laws that translate into rules the customs and values of the past and present."

A weighing of values is an inescapable part in the interpretation and growth of the Fourth Amendment. Expectations, and their reasonableness, vary according to circumstances. So will the need for an intrusion and its likely effect. These elements will define the boundaries of the interests which the Amendment holds as "secure."

To identify the interests which are to be "secure," of course, only begins the inquiry. It is equally essential to identify the dangers from which those interests are to be secure. What constitutes an intrusion will depend on the scope of the protected interest. The early view that the Fourth Amendment protected only tangible property resulted in the rule that a physical trespass or taking was the measure of an intrusion. *Olmstead* rested on the fact that there had been no physical trespass into the defendant's home or office. It also held that the use of the sense of hearing to intercept a conversation did not constitute a search or seizure. *Katz*, by expanding the scope of the protected interests, necessarily altered our misunderstanding of what constitutes an intrusion. Since intangibles such as oral conversations are now regarded as protected "effects," the overhearing of a conversation may constitute an intrusion apart from whether a physical trespass is involved.

The nature of the search and seizure can be very important. An entry into a house to search its interior may be viewed as more serious than the overhearing of a certain type of conversation. The risk of abuse may loom larger in one case than the other. The factors that have come to be viewed as most important, however, are the purpose and effect of the intrusion. The Supreme Court has tended to focus not so much on what was physically done, but on why it was done and what the consequence is likely to be. What is seized, why it was seized, and what is done with what is seized are critical questions.

I stated earlier that a central concern of the Fourth Amendment was with intrusions to obtain evidence to incriminate the victim of the search. This concern has been reflected in Supreme Court decisions which have traditionally

treated intrusions to gather incriminatory evidence differently from intrusions for neutral or benign purposes. In *Frank v. Maryland*, the appellant was fined for refusing to allow a housing inspector to enter his residence to determine whether it was maintained in compliance with the municipal housing code. Violation of the code would have led only to a direction to remove the violation. Only failure to comply with the direction would lead to a criminal sanction. The Court held that such administrative searches could be conducted without warrant. Justice Frankfurter, writing for the Court, noted that the Fourth Amendment was a reaction to "ransacking by Crown officers of the homes of citizens in search of evidence of crime or of illegally imported goods." He observed that both *Entick* and *Boyd* were concerned with attempts to compel individuals to incriminate themselves in criminal cases and that "it was on the issue of the right to be secure from searches for evidence to be used in criminal prosecutions or for forfeitures that the great battle for fundamental liberty was fought." There was thus a great difference, the Justice said, between searches to seize evidence for criminal prosecutions and searches to detect the existence of municipal health code violations. Searches in this latter category, conducted "as an adjunct to a regulatory scheme for the general welfare of the community and not as a means of enforcing the criminal law, [have] antecedents deep in our history," and should not be subjected to the warrant requirement.

*Frank* was later overruled in 1967 in *Camara v. Municipal Court*, and a companion case, *See v. City of Seattle*. In *Camara*, appellant was, like *Frank*, charged with a criminal violation as a result of his refusal to permit a municipal inspector to enter his apartment to investigate possible violations of the city's housing code. The Supreme Court rejected the *Frank* rationale that municipal fire, health, and housing inspections could be conducted without a warrant because the object of the intrusion was not to search for the fruits or instrumentalities of crime. Moreover, the Court noted that most regulatory laws such as fire, health, and housing codes were enforced by criminal processes, that refusal to permit entry to an inspector was often a criminal offense, and that the "self-protection" or "non-incrimination" objective of the Fourth Amendment was therefore indeed involved.

But the doctrine of *Camara* proved to be limited. In 1971 in *Wyman v. James* the Court held that a "home visit" by a welfare caseworker, which entailed termination of benefits if the welfare recipient refused entry, was lawful despite the absence of a warrant. The Court relied on the importance of the public's interest in obtaining information about the recipient, the reasonableness of the measures taken to ensure that the intrusion was limited to the extent practicable, and most importantly, the fact that the primary objective of the search was not to obtain evidence for a criminal investigation or prosecution. *Camara* and *Frank* were distinguished as involving criminal proceedings.

Perhaps what these cases mainly say is that the purpose of the intrusion, and the use to which what is seized is put, are more important from a constitutional standpoint than the physical act of intrusion itself. Where the purpose or effect is noncriminal, the search and seizure is perceived as less troublesome and there is a readiness to find reasonableness even in the absence of a judicial warrant. By contrast, where the purpose of the intrusion is to gather incriminatory evidence, and hence hostile, or when the consequence of the intrusion is the sanction of the criminal law, greater protections may be given.

The Fourth Amendment then, as it has always been interpreted, does not give absolute protection against Government intrusion. In the words of the Amendment, the right guaranteed is security against *unreasonable* searches and seizures. As Justice White said in the *Camara* case, "there can be no ready test for determining reasonableness other than by balancing the need to search against the invasion which the search entails." Whether there has been a constitutionally prohibited invasion at all has come to depend less on an absolute dividing line between protected and unprotected areas, and more on an estimation of the individual security interests affected by the Government's actions. Those effects, in turn, may depend on the purpose for which the search is made, whether it is hostile, neutral, or benign in relation to the person whose interests are invaded, and also on the manner of the search.

By the same token, the Government's need to search, to invade individual privacy interests, is no longer measured exclusively—if indeed it ever was—by the traditional probable cause standard. The second clause of the Amendment states, in part, that "no warrants shall issue but upon probable cause." The concept of probable cause has often been read to bear upon and in many cases

to control the question of the reasonableness of searches, whether with or without warrant. The traditional formulation of the standard, as "reasonable grounds for believing that the law was being violated on the premises to be searched" relates to the Governmental interest in the prevention of criminal offenses, and to seizure of their instruments and fruits (*Brinegar v. United States*). This formulation in *Gouled v. United States* once took content from the long-standing "mere evidence rule"—that searches could not be undertaken "solely for the purpose of . . . [securing] evidence to be used . . . in a criminal or penal proceeding, but that they may be resorted to only when a primary right to such search and seizure may be found in the interest which the public . . . may have in the property to be seized." The Government's interest in the intrusion, like the individual's interest in privacy, thus was defined in terms of property, and the right to search as well as to seize was limited to items—contraband and the fruits and instrumentalities of crime—in which the Government's interest was thought superior to the individual's. This notion, long eroded in practice, was expressly abandoned by the Court in 1967 in *Warden v. Hayden*. Thus, the detection of crime—the need to discover and use "mere evidence"—may presently justify intrusion.

Moreover, as I have indicated, the Court has held that, in certain situations, something less than probable cause—in the traditional sense—may be sufficient ground for intrusion, if the degree of intrusion is limited strictly to the purposes for which it is made. In *Terry v. Ohio* the Court held that a policeman, in order to protect himself and others nearby, may conduct a limited "pat down" search for weapons when he has reasonable grounds for believing that criminal conduct is taking place and that the person searched is armed and dangerous. Last term, in *United States v. Brignoni-Ponce*, the Court held that, if an officer has a "founded suspicion" that a car in a border area contains illegal aliens, the officer may stop the car and ask the occupants to explain suspicious circumstances. The Court concluded that the important Governmental interest involved, and the absence of practical alternatives, justified the minimal intrusion of a brief stop. In both *Terry* and *Brignoni*, the Court emphasized that a more drastic intrusion—a thorough search of the suspect or automobile—would require the justification of traditional probable cause. This point is reflected in the Court's decisions in *Almeida-Sánchez* and *Ortiz*, in which the Court held that, despite the interest in stemming illegal immigration, searches of automobiles either at fixed checkpoints or by roving patrols in places that are not the "functional equivalent" of borders could not be undertaken without probable cause.

Nonetheless, it is clear that the traditional probable cause standard is not the exclusive measure of the Government's interest. The kind and degree of interest required depend on the severity of the intrusion the Government seeks to make. The requirement of the probable cause standard itself may vary, as the Court made clear in *Camara*. That case, as you recall, concerned the nature of the probable cause requirement in the context of searches to identify housing code violations. The Court was persuaded that the only workable method of enforcement was periodic inspection of all structures, and concluded that because the search was not "personal in nature," and the invasion of privacy involved was limited, probable cause could be based on "appraisal of conditions in the area as a whole," rather than knowledge of the condition of particular buildings. "If a valid public interest justifies the intrusion contemplated," the court stated, "then there is probable cause to issue a suitable restricted search warrant." In the *Keith* case, while holding that domestic national security surveillance—not involving the activities of foreign powers and their agents—was subject to the warrant requirement, the Court noted that the reasons for such domestic surveillance may differ from those justifying surveillances for ordinary crimes, and that domestic security surveillances often have to be long range projects. For these reasons, a standard of probable cause to obtain a warrant different from the traditional standard would be justified: "Different standards may be compatible with the Fourth Amendment if they are reasonable both in relation to the legitimate need of Government for intelligence information and the protected rights of our citizens."

In brief, although at one time the "reasonableness" of a search may have been defined according to the traditional probable cause standard, the situation has now been reversed. Probable cause has come to depend on reasonableness—on the legitimate need of the Government and whether there is reason to believe that the precise intrusion sought, measured in terms of its effect on individual security, is necessary to satisfy it.

This point is critical in evaluating the reasonableness of searches or surveillances undertaken to protect national security. In some instances, the Government's interest may be, in part, to protect the nation against specific actions of foreign powers or their agents—actions that are criminal offenses. In other instances, the interest may be to protect against the possibility of actions by foreign powers and their agents dangerous to national security—actions that may or may not be criminal. Or the interest may be solely to gather intelligence, in a variety of forms, in the hands of foreign agents and foreign powers—intelligence that may be essential to informed conduct of our nation's foreign affairs. This last interest indeed may often be far more critical for the protection of the nation than the detection of a particular criminal offense. The Fourth Amendment's standard of reasonableness as it has developed in the Court's decisions is sufficiently flexible to recognize this.

Just as the reasonableness standard of the Amendment's first clause has taken content from the probable cause standard, so it has also come to incorporate the particularity requirement of the warrant clause—that warrants particularly describe “the place to be searched, and the persons or things to be seized.” As one Circuit Court has written, in *United States v. Poller*, although pointing out the remedy might not be very extensive, “[L]imitations on the fruit to be gathered tend to limit the quest itself.”

The Government's interest and purpose in undertaking the search defines its scope, and the societal importance of that purpose can be weighed against the effects of the intrusion on the individual. By precise definition of the objects of the search, the degree of intrusion can be minimized to that reasonably necessary to achieve the legitimate purpose. In this sense, the particularity requirement of the warrant clause is analogous to the minimization requirement of Title III, that interceptions “be executed in such a way to minimize the interception of communications not otherwise subject to interception” under the Title.

But there is a distinct aspect to the particularity requirements—one that is often overlooked. An officer who has obtained a warrant based upon probable cause to search for particular items may in conducting the search necessarily have to examine other items, some of which may constitute evidence of an entirely distinct crime. The normal rule under the plain view doctrine is that the officer may seize the latter incriminating items as well as those specifically identified in the warrant so long as the scope of the authorized search is not exceeded. The minimization rule responds to the concern about overly broad searches, and it requires an effort to limit what can be seized. It also may be an attempt to limit how it can be used. Indeed, this minimization concern may have been the original purpose of the “mere evidence” rule.

The concern about the use of what is seized may be most important for future actions. Until very recently—in fact, until the Court's 1971 decision in *Bivens v. Six Unknown Federal Narcotic Agents*—the only sanction against an illegal search was that its fruits were inadmissible at any criminal trial of the person whose interest was invaded. So long as this was the only sanction, the courts, in judging reasonableness, did not really have to weigh any governmental interest other than that of detecting crimes. In practical effect, a search could only be “unreasonable” as a matter of law if an attempt was made to use its fruits for prosecution of a criminal offense. So long as the Government did not attempt such use, the search could continue and the Government's interests, other than enforcing criminal laws, could be satisfied.

It may be said that this confuses rights and remedies; searches could be unreasonable even though no sanction followed. But I am not clear that this is theoretically so, and realistically it was not so. As I have noted earlier, the reasonableness of a search has depended, in major part, on the purpose for which it is undertaken and on whether that purpose, in relation to the person whom it affects, is hostile or benign. The search most hostile to an individual is one in preparation for his criminal prosecution. Exclusion of evidence from criminal trials may help assure that searches undertaken for ostensibly benign motives are not used as blinds for attempts to find criminal evidence, while permitting searches that are genuinely benign to continue. But there is a more general point. The effect of a Government intrusion on individual security is a function, not only of the intrusion's nature and circumstances, but also of disclosure and of the use to which its product is put. Its effects are perhaps greatest when it is employed or can be employed to impose criminal sanctions or to deter, by disclosure, the exercise of individual freedoms. In short, the use of the product seized bears upon the reasonableness of the search.

"These observations have particular bearing on electronic surveillance. By the nature of the technology the "search" may necessarily be far broader than its legitimate objects. For example, a surveillance justified as the only means of obtaining value foreign intelligence may require the temporary overhearing of conversations containing no foreign intelligence whatever in order eventually to locate its object. To the extent that we can, by purely mechanical means, select out only that information that fits the purpose of the search, the intrusion is radically reduced. Indeed, in terms of effects on individual security, there would be no intrusion at all. But other steps may be appropriate. In this respect, I think we should recall the language and the practice for many years under former § 605 of the Communications Act. The Act was violated, not by surveillance alone, but only by surveillance *and* disclosure in court or to the public. It may be that if a critical Governmental purpose justifies a surveillance, but because of technological limitations it is not possible to limit surveillance strictly to those persons as to whom alone surveillance is justified, one way of reducing the intrusion's effects is to limit strictly the revelation or disclosure or the use of its product. Minimization procedures can be very important.

In discussing the standard of reasonableness, I have necessarily described the evolving standards for issuing warrants and the standards governing their scope. But I have not yet discussed the warrant requirement itself—how it relates to the reasonableness standard and what purposes it was intended to serve. The relationship of the warrant requirement to the reasonableness standard was described in *Johnson v. United States* by Justice Robert Jackson: "Any assumption that evidence sufficient to support a magistrate's disinterested determination to issue a search warrant will justify the officers in making a search without a warrant would reduce the Amendment to a nullity and leave the people's homes secure only in the discretion of police officers. . . . When the rights of privacy must reasonably yield to the right of search is, as a rule, to be decided by a judicial officer, not by a policeman or government enforcement agent. This view has not always been accepted by a majority of the Court; the Court's view of the relationship between the general reasonableness standard and the warrant requirement has shifted often and dramatically. But the view expressed by Justice Jackson is now quite clearly the prevailing position. The Court said in *Katz* that "searches conducted outside the judicial process, without prior approval by judge or magistrate, are *per se* unreasonable under the Fourth Amendment—subject only to a few specifically established and well-delineated exceptions." Such exceptions include those grounded in necessity—where exigencies of time and circumstance make resort to a magistrate practically impossible. These include, of course, the *Terry* stop and frisk and, to some degree, searches incident to arrest. But there are other exceptions, not always grounded in exigency—for example, some automobile searches—and at least some kinds of searches not conducted for purposes of enforcing criminal laws—such as the welfare visits of *Wyman v. James*. In short, the warrant requirement itself depends on the purpose and degree of intrusion. A footnote to the majority opinion in *Katz*, as well as Justice White's concurring opinion, left open the possibility that warrants may not be required for searches undertaken for national security purposes. And, of course, Justice Powell's opinion in *Keith*, while requiring warrants for domestic security surveillances, suggests that a different balance may be struck when the surveillance is undertaken against foreign powers and their agents to gather intelligence information or to protect against foreign threats.

The purpose of the warrant requirement is to guard against over-zealousness of Government officials, who may tend to overestimate the basis and necessity of intrusion and to underestimate the impact of their efforts on individuals. It was said in *United States v. United States District Court*: "The historical judgment, which the Fourth Amendment accepts, is that unreviewed executive discretion may yield too readily to pressures to obtain incriminating evidence and overlook potential invasions of privacy and protected speech." These purposes of the warrant requirement must be kept firmly in mind in analyzing the appropriateness of applying it to the foreign intelligence and security area.

There is a real possibility that application of the warrant requirement, at least in the form of the normal criminal search warrant, the form adopted in Title III, will endanger legitimate Government interests. As I have indicated, Title III sets up a detailed procedure for interception of wire or oral communications. It requires the procurement of a judicial warrant and prescribes the information to be set forth in the petition to the judge so that, among other things, he may find probable cause that a crime has been or is about to be committed. It re-

quires notification to the parties subject to the surveillance within a period after it has taken place. The statute is clearly unsuited to protection of the vital national interests in continuing detection of the activities of foreign powers and their agents. A notice requirement—aside from other possible repercussions—could destroy the usefulness of intelligence sources and methods. The most critical surveillance in this area may have nothing whatever to do with detection of crime.

Apart from the problems presented by particular provisions of Title III, the argument against application of the warrant requirement, even with an expanded probable cause standard, is that judges and magistrates may underestimate the importance of the Government's need, or that the information necessary to make that determination cannot be disclosed to a judge or magistrate without risk of its accidental revelation—a revelation that could work great harm to the nation's security. What is often less likely to be noted is that a magistrate may be as prone to overestimate as to underestimate the force of the Government's need. Warrants necessarily are issued *ex parte*; often decision must come quickly on the basis of information that must remain confidential. Applications to any one judge or magistrate would be only sporadic; no opinion could be published: this would limit the growth of judicially developed, reasonably uniform standards based, in part, on the quality of the information sought and the knowledge of possible alternatives. Equally important, responsibility for the intrusion would have been diffused. It is possible that the actual number of searches or surveillances would increase if executive officials, rather than bearing responsibility themselves, can find shield behind a magistrate's judgment of reasonableness. On the other hand, whatever the practical effect of a warrant requirement may be, it would still serve the important purpose of assuring the public that searches are not conducted without the approval of a neutral magistrate who could prevent abuses of the technique.

In discussing the advisability of a warrant requirement, it may also be useful to distinguish among possible situations that arise in the national security area. Three situations—greatly simplified—come to mind. They differ from one another in the extent to which they are limited in time or in target. First, the search may be directed at a particular foreign agent to detect a specific anticipated activity—such as the purchase of a secret document. The activity which is to be detected ordinarily would constitute a crime. Second, the search may be more extended in time—even virtually continuous—but still would be directed at an identified foreign agent. The purpose of such a surveillance would be to monitor the agent's activities, determine the identities of persons whose access to classified information he might be exploiting, and determine the identity of other foreign agents with whom he may be in contact. Such a surveillance might also gather foreign intelligence information about the agent's own country, information that would be of positive intelligence value to the United States. Third, there may be virtually continuous surveillance which by its nature does not have specifically predetermined targets. Such a surveillance could be designed to gather foreign intelligence information essential to the security of the nation.

The more limited in time and target a surveillance is, the more nearly analogous it appears to be with a traditional criminal search which involves a particular target location or individual at a specific time. Thus, the first situation I just described would in that respect be most amenable to some sort of warrant requirement, the second less so. The efficiency of a warrant requirement in the third situation would be minimal. If the third type of surveillance I described were submitted to prior judicial approval, that judicial decision would take the form of an *ex parte* declaration that the program of surveillance designed by the Government strikes a reasonable balance between the government's need for the information and the protection of individuals' rights. Nevertheless, it may be that different kinds of warrants could be developed to cover the third situation. In his opinion in *Almeida-Sánchez*, Justice Powell suggested the possibility of area warrants—issued on the basis of the conditions in the area to be surveilled—to allow automobile searches in areas near America's borders. The law has not lost its inventiveness, and it might be possible to fashion new judicial approaches to the novel situations that come up in the area of foreign intelligence. I think it must be pointed out that for the development of such an extended, new kind of warrant, a statutory base might be required or at least appropriate. At the same time, in dealing with this area,

it may be mistaken to focus on the warrant requirement alone to the exclusion of other, possibly more realistic, protections.

What, then, is the shape of the present law? To begin with, several statutes appear to recognize that the Government does intercept certain messages for foreign intelligence purpose and that this activity must be, and can be, carried out. Section 952 of Title 18, which I mentioned earlier is one example; section 798 of the same title is another. In addition, Title III's proviso, which I have quoted earlier, explicitly disclaimed any intent to limit the authority of the Executive to conduct electronic surveillance for national security and foreign intelligence purposes. In an apparent recognition that the power would be exercised, Title III specifies the conditions under which information obtained through Presidential authorized surveillance may be received into evidence. It seems clear, therefore, that in 1968 Congress was not prepared to come to a judgment that the Executive should discontinue its activities in this area, nor was it prepared to regulate how those activities were to be conducted. Yet it cannot be said that Congress has been entirely silent on this matter. Its express statutory references to the existence of the activity must be taken into account.

The case law, although unsatisfactory in some respects, has supported or left untouched the policy of the Executive in the foreign intelligence area whenever the issue has been squarely confronted. The Supreme Court's decision in the *Keith* case in 1972 concerned the legality of warrantless surveillance directed against a domestic organization with no connection to a foreign power and the Government's attempt to introduce the product of the surveillance as evidence in the criminal trial of a person charged with bombing a C.I.A. office in Ann Arbor, Michigan. In part because of the danger that uncontrolled discretion might result in use of electronic surveillance to deter domestic organizations from exercising First Amendment rights, the Supreme Court held that in cases of internal security, when there is no foreign involvement, a judicial warrant is required. Speaking for the Court, Justice Powell emphasized that "this case involves only the domestic aspects of national security. We have expressed no opinion as to the issues which may be involved with respect to activities of foreign powers or their agents."

As I observed in my remarks at the ABA convention, the Supreme Court surely realized, "in view of the importance the Government has placed on the need for warrantless electronic surveillance that, after the holding in *Keith*, the Government would proceed with the procedures it had developed to conduct those surveillances not prohibited—that is, in the foreign intelligence area or, as Justice Powell said, 'with respect to activities of foreign powers and their agents.'"

The two federal circuit court decisions after *Keith* that have expressly addressed the problem have both held that the Fourth Amendment does not require a warrant for electronic surveillance instituted to obtain foreign intelligence. In the first, *United States v. Brown* the defendant, an American citizen, was incidentally overheard as the result of a warrantless wiretap authorized by the Attorney General for foreign intelligence purposes. In upholding the legality of the surveillance, the Court of Appeals for the Fifth Circuit declared that on the basis of "the President's constitutional duty to act for the United States in the field of foreign affairs, and his inherent power to protect national security in the conduct of foreign affairs . . . the President may constitutionally authorize warrantless wiretaps for the purpose of gathering foreign intelligence." The court added that "(r)estrictions on the President's power which are appropriate in cases of domestic security become inappropriate in the context of the international sphere."

In *United States v. Butenko* the Third Circuit reached the same conclusion—that the warrant requirement of the Fourth Amendment does not apply to electronic surveillance undertaken for foreign intelligence purposes. Although the surveillance in that case was directed at a foreign agent, the court held broadly that the warrantless surveillance would be lawful so long as the primary purpose was to obtain foreign intelligence information. The court stated that such surveillance would be reasonable without a warrant even though it might involve the overhearing of conversations of "alien officials and agents, and perhaps of American citizens." I should note that although the United States prevailed in the *Butenko* case, the Department acquiesced in the petitioner's application for *cetiorari* in order to obtain the Supreme Court's ruling on the question. The Supreme Court denied review, however, and thus left the Third Circuit's decision undisturbed as the prevailing law.

Most recently, in *Zweibon v. Mitchell*, decided in June of this year, the District of Columbia Circuit dealt with warrantless electronic surveillance directed against a domestic organization allegedly engaged in activities affecting this country's relations with a foreign power. Judge Skelly Wright's opinion for four of the nine judges makes many statements questioning any national security exception to the warrant requirement. The court's actual holding made clear in Judge Wright's opinion was far narrower and, in fact, is consistent with holdings in *Brown* and *Butenko*. The court held only that "a warrant must be obtained before a wiretap is installed on a domestic organization that is neither the agent of nor acting in collaboration with a foreign power." This holding, I should add, was fully consistent with the Department of Justice's policy prior to the time of the *Zweibon* decision.

With these cases in mind, it is fair to say electronic surveillance conducted for foreign intelligence purposes, essential to the national security, is lawful under the Fourth Amendment, even in the absence of a warrant, at least where the subject of the surveillance is a foreign power or an agent or collaborator of a foreign power. Moreover, the opinions of two circuit courts stress the purpose for which the surveillance is undertaken, rather than the identity of the subject. This suggests that in their view such surveillance without a warrant is lawful so long as its purpose is to obtain foreign intelligence.

But the legality of the activity does not remove from the Executive or from Congress the responsibility to take steps, within their power, to seek an accommodation between the vital public and private interests involved. In our effort to seek such an accommodation, the Department has adopted standards and procedures designed to ensure the reasonableness under the Fourth Amendment of electronic surveillance and to minimize to the extent practical the intrusion on individual interests. As I have stated, it is the Department's policy to authorize electronic surveillance for foreign intelligence purposes only when the subject is a foreign power or an agent of a foreign power. By the term "agent" I mean a conscious agent; the agency must be of a special kind and must relate to activities of great concern to the United States for foreign intelligence or counter-intelligence reasons. In addition, at present, there is no warrantless electronic surveillance directed against any American citizen, and although it is conceivable that circumstances justifying such surveillance may arise in the future, I will not authorize the surveillance unless it is clear that the American citizen is an active, conscious agent or collaborator of a foreign power. In no event, of course, would I authorize any warrantless surveillance against domestic persons or organizations such as those involved in the *Keith* case. Surveillance without a warrant will not be conducted for purposes of security against domestic or internal threats. It is our policy, moreover, to use the Title III procedure whenever it is possible and appropriate to do so, although the statutory provisions regarding probable cause, notification, and prosecutive purpose make it unworkable in all foreign intelligence and many counterintelligence cases.

The standards and procedures that the Department has established within the United States seek to ensure that every request for surveillance receives thorough and impartial consideration before a decision is made whether to institute it. The process is elaborate and time-consuming, but it is necessary if the public interest is to be served and individual rights safeguarded.

I have just been speaking about telephone wiretapping and microphone surveillances which are reviewed by the Attorney General. In the course of its investigation, the committee has become familiar with the more technologically sophisticated and complex electronic surveillance activities of other agencies. These surveillance activities present somewhat different legal questions. The communications conceivably might take place entirely outside the United States. That fact alone, of course, would not automatically remove the agencies' activities from scrutiny under the Fourth Amendment since at times even communications abroad may involve a legitimate privacy interest of American citizens. Other communications conceivably might be exclusively between foreign powers and their agents and involve no American terminal. In such a case, even though American citizens may be discussed, this may raise less significant, or perhaps no significant, questions under the Fourth Amendment. But the primary concern, I suppose, is whether reasonable minimization procedures are employed with respect to use and dissemination.

With respect to all electronic surveillance, whether conducted within the United States or abroad, it is essential that efforts be made to minimize as much as possible the extent of the intrusion. Much in this regard can be done

by modern technology. Standard and procedures can be developed and effectively deployed to limit the scope of the intrusion and the use to which its product is put. Various mechanisms can provide a needed assurance to the American people that the activity is undertaken for legitimate foreign intelligence purposes, and not for political or other improper purposes. The procedures used should not be ones which by indirection in fact target American citizens and resident aliens where these individuals would not themselves be appropriate targets. The proper minimization criteria can limit the activity to its justifiable and necessary scope.

Another factor must be recognized. It is the importance or potential importance of the information to be secured. The activity may be undertaken to obtain information deemed necessary to protect the nation against actual or potential attack or other hostile acts of a foreign power, to obtain intelligence information deemed essential to the security of the United States, or to protect national security information against foreign intelligence activities.

Need is itself a matter of degree. It may be that the importance of some information is slight, but that may be impossible to gauge in advance; the significance of a single bit of information may become apparent only when joined to intelligence from other sources. In short, it is necessary to deal in probabilities. The importance of information gathered from foreign establishments and agents may be regarded generally as high—although even here there may be wide variations. At the same time, the effect on individual liberty and security—at least of American citizens—caused by methods directed exclusively to foreign agents, particularly with minimization procedures, would be very slight.

There may be regulatory and institutional devices other than the warrant requirement that would better assure that intrusions for national security and foreign intelligence purposes reasonably balance the important needs of Government and of individual interests. In assessing possible approaches to this problem it may be useful to examine the practices of other Western democracies. For example, England, Canada, and West Germany each share our concern about the confidentiality of communications within their borders. Yet each recognizes the right of the Executive to intercept communications without a judicial warrant in cases involving suspected espionage, subversion or other national security intelligence matters.

In Canada and West Germany, which have statutes analogous to Title III, the Executive in national security cases is exempt by statute from the requirement that judicial warrants be obtained to authorize surveillance of communications. In England, where judicial warrants are not required to authorize surveillance of communications in criminal investigations, the relevant statutes recognize an inherent authority in the Executive to authorize such surveillance in national security cases.<sup>3</sup> In each country, this authority is deemed to cover interception of mail and telegrams, as well as telephone conversations.

In all three countries, requests for national security surveillance may be made by the nation's intelligence agencies. In each, a Cabinet member is authorized to grant the request.

In England and West Germany, however, interception of communications is intended to be a last resort, used only when the information being sought is likely to be unobtainable by any other means. It is interesting to note, however, that both Canada and West Germany do require the Executive to report periodically to the Legislature on its national security surveillance activities. In Canada, the Solicitor General files an annual report with the Parliament setting forth the number of national security surveillances initiated, their average length, a general description of the methods of interception or seizure used, and assessment of their utility.

It may be that we can draw on these practices of other Western democracies, with appropriate adjustments to fit our system of separation of powers. The procedures and standards that should govern the use of electronic methods of obtaining foreign intelligence and of guarding against foreign threats are matters of public policy and values. They are of critical concern to the Executive Branch and to Congress, as well as to the courts. The Fourth Amendment itself is a reflection of public policy and values—an evolving accommodation between governmental needs and the necessity of protecting individual security and rights.

---

<sup>3</sup> Report of the Committee of Privy Councillors appointed to inquire into the interception of communications (1957), which states, at page 5, that, "The origin of the power to intercept communications can only be surmised, but the power has been exercised from very early times; and has been recognised as a lawful power by a succession of statutes covering the last 200 years or more."

General public understanding of these problems is of paramount importance, to assure that neither the Executive, nor the Congress, nor the courts risk discounting the vital interests on both sides.

The problems are not simple. Evolving solutions probably will and should come—as they have in the past—from a combination of legislation, court decisions, and executive actions. The law in this area, as Lord Devlin once described the law of search in England, “is haphazard and ill defined.” It recognized the existence and the necessity of the Executive’s power. But the Executive and the Legislature are, as Lord Devlin also said, “expected to act reasonably.” The future course of the law will depend on whether we can meet that obligation.

#### **TESTIMONY OF HON. EDWARD H. LEVI, ATTORNEY GENERAL OF THE UNITED STATES**

Attorney General Levi. I must warn that even the truncated version, unfortunately, is long.

I am here today, Mr. Chairman, in response to a request from the committee to discuss the relationship between electronic surveillance and the fourth amendment of the Constitution. If I remember correctly, the original request was that I place before the committee the philosophical or jurisprudential framework relevant to this relationship which lawyers, viewing this complex field, ought to keep in mind. If this sounds vague and general and perhaps useless, I can only ask for indulgence. My first concern when I received the request was that any remarks I might be able to make would be so general as not to be helpful to the committee. But I want to be as helpful to the committee as I can be.

The area with which the committee is concerned is a most important one. In my view, the development of the law in this area has not been satisfactory, although there are reasons why the law has developed as it has. Improvement of the law, which in part means its clarification, will not be easy. Yet it is a most important venture. In a talk before the American Bar Association last August, I discussed some of the aspects of the legal framework. Speaking for the Department of Justice, I concluded this portion of the talk with the observation and commitment that “we have very much in mind the necessity to determine what procedures through legislation, court action or executive processes will best serve the national interest, including, of course, the protection of constitutional rights.”

I begin then with an apology for the general nature of my remarks. This will be due in part to the nature of the law itself in this area. But I should state at the outset there are other reasons as well. In any area, and possibly in this one more than most, legal principles gain meaning through an interaction with the facts. Thus, the factual situations to be imagined are of enormous significance.

As this committee well knows, some of the factual situations to be imagined in this area are not only of a sensitive nature but also of a changing nature. Therefore, I am limited in what I can say about them, not only because they are sensitive, but also because a lawyer’s imagination about future scientific developments carries its own warnings of ignorance. This is a point worth making when one tries to develop appropriate safeguards for the future.

There is an additional professional restriction upon me which I am sure the committee will appreciate. The Department of Justice has under active criminal investigation various activities which may or

may not have been illegal. In addition, the Department through its own attorneys, or private attorneys specially hired, is representing present or former Government employees in civil suits which have been brought against them for activities in the course of official conduct. These circumstances naturally impose some limitation upon what it is appropriate for me to say in this forum. I ought not give specific conclusory opinions as to matters under criminal investigation or in litigation. I can only hope that what I have to say may nevertheless be of some value to the committee in its search for constructive solutions.

I do realize there has to be some factual base, however unfocused it may at times have to be, to give this discussion meaning. Therefore, as a beginning, I propose to recount something of the history of the Department's position and practice with respect to the use of electronic surveillance, both for telephone wiretapping and for trespassory placement of microphones.

As I read the history, going back to 1931 and undoubtedly prior to that time, except for an interlude between 1928 and 1931 and for 2 months in 1940, the policy of the Department of Justice has been that electronic surveillance could be employed without a warrant in certain circumstances. During the rest of the thirties it appears that the Department's policy concerning telephone wiretapping generally conformed to the guidelines adopted by Attorney General William Mitchell. Telephone wiretapping was limited to cases involving the safety of the victim, as in kidnapings, location and apprehension of "desperate" criminals, and other cases considered to be of major law enforcement importance, such as espionage and sabotage.

In December 1937, however, in the first *Nardone* case, the United States Supreme Court reversed the Court of Appeals for the Second Circuit, and applied section 605 of the Federal Communications Act of 1934 to law enforcement officers; thus rejecting the Department's argument that it did not so apply. Although the Court read the act to cover only wire interceptions where there had also been disclosure in court or to the public, the decision undoubtedly had its impact upon the Department's estimation of the value of telephone wiretapping as an investigative technique. In the second *Nardone* case in December 1939, the act was read to bar the use in court not only of the overhead evidence, but also the fruits of that evidence. Possibly for this reason, and also because of public concern over telephone wiretapping, on March 15, 1940, Attorney General Robert Jackson imposed a total ban on its use for the Department. This ban lasted about 2 months.

On May 21, 1940, President Franklin Roosevelt issued a memorandum to the Attorney General stating his view that electronic surveillance would be proper under the Constitution where "grave matters involving defense of the nation" were involved. The President authorized and directed the Attorney General "to secure information by listening devices [directed at] the conversation or other communications of persons suspected of subversive activities against the Government of the United States, including suspected spies." The Attorney General was requested "to limit these investigations so conducted to a minimum and to limit them insofar as possible to aliens." Although the President's memorandum did not use the term "trespassory microphone surveillance," the language was sufficiently broad

to include that practice, and the Department construed it as an authorization to conduct trespassory microphone surveillances as well as telephone wiretapping in national security cases. The authority for the President's action was later confirmed by an opinion by Assistant Solicitor General Charles Fahy who advised the Attorney General that electronic surveillance could be conducted where matters affected the security of the Nation.

On July 17, 1946, Attorney General Tom C. Clark sent President Truman a letter reminding him that President Roosevelt had authorized and directed Attorney General Jackson to approve "listening devices [directed at] the conversation of other communications of persons suspected of subversive activities against the Government of the United States, including suspected spies."

The CHAIRMAN. Mr. Attorney General, you're referring by that term "trespassory microphone surveillance" to bugs, are you not?

Attorney General LEVI. Well—

The CHAIRMAN. Bugs and wiretaps?

Attorney General LEVI. That is one way they are commonly referred to.

The CHAIRMAN. Yes, thank you.

Attorney General LEVI. And that the directive had been followed by Attorneys General Robert Jackson and Francis Biddle. Attorney General Clark recommended that the directive "be continued in force" in view of the "increase in subversive activities" and "a very substantial increase in crime." He stated that it was imperative to use such techniques "in cases vitally affecting the domestic security, or where human life is in jeopardy" and that Department files indicated that his two most recent predecessors as Attorney General would concur in this view. President Truman signed his concurrence on the Attorney General's letter.

In 1952, there were 285 telephone wiretaps, 300 in 1953, and 322 in 1954. Between February 1952 and May 1954, the Attorney General's position was not to authorize trespassory microphone surveillance. This was the position taken by Attorney General McGrath, who informed the FBI that he would not approve the installation of trespassory microphone surveillance because of his concern over a possible violation of the fourth amendment.

Nevertheless, FBI records indicate there were 63 microphones installed in 1952, there were 52 installed in 1953, and there were 99 installed in 1954.

The CHAIRMAN. Was that during Attorney General McGrath's period in office?

Attorney General LEVI. Yes.

The CHAIRMAN. Are you saying then that his orders were disregarded by the FBI?

Attorney General LEVI. I may not be saying that because, as I think the statement will show, there may well have been a view that the approval of the Attorney General was not required. It may be that Attorney General McGrath was simply saying that he would not give his approval, but he may not have been prohibiting the use.

I cannot answer the question better than that.

Senator MATHIAS. Mr. Chairman, the Attorney General has relied upon the views of his predecessors in stating the position of the De-

partment. Perhaps it is not inappropriate to comment that some of his predecessors, as advocates, did have the view that he is purporting. But later when they went to the Supreme Court, in a more neutral and objective position, they changed their views and Attorney General Jackson and Attorney General Clark had that experience. The elevation of defense seemed to give them a different perspective.

Attorney General LEVI. This committee, of course, has an enormous number of documents from the Department of Justice. You may have seen more than I have seen, although I doubt it on this point.

Senator MATHIAS. I do not dispute your reflection of their views as Attorneys General. I am just saying that not only this committee but the Justice Department has copies of Supreme Court opinions where they registered different views.

Attorney General LEVI. I think that the responsibility often determines action. It is also true that when one speaks of Attorney General Jackson, I think he was unique in that his attitude was that he only became a free man when he went on the Supreme Court. That is not a position which I think other people should take, and I always thought it was rather astonishing that he took it.

To continue, the policy against Attorney General approval, at least in general, of trespassory microphone surveillance was reversed by Attorney General Herbert Brownell on May 20, 1954, in a memorandum to Director Hoover instructing him that the Bureau was authorized to conduct trespassory microphone surveillances. The Attorney General stated that:

Considerations of internal security and the national safety are paramount and, therefore, may compel the unrestricted use of this technique in the national interest.

A memorandum from Director Hoover to the Deputy Attorney General on May 4, 1961, described the Bureau's practice since 1954 as follows:

In the internal security field, we are utilizing microphone surveillances on a restricted basis even though trespass is necessary to assist in uncovering the activities of Soviet intelligence agents and Communist Party leaders. In the interests of national safety, microphone surveillances are also utilized on a restricted basis, even though trespass is necessary, in uncovering major criminal activities. We are using such coverage in connection with our investigations of the clandestine activities of top hoodlums and organized crime. From an intelligence standpoint, this investigative technique has produced results unobtainable through other means. The information so obtained is treated in the same manner as information obtained from wiretaps, that is, not from the standpoint of evidentiary value but for intelligence purposes.

President Johnson announced a policy for Federal agencies in June 1965, which required that the interception of telephone conversations without the consent of one of the parties be limited to investigations relating to national security and that the consent of the Attorney General be obtained in each instance. The memorandum went on to state that use of mechanical or electronic devices to overhear conversations not communicated by wire is an even more difficult problem "which raised substantial and unresolved questions of Constitutional interpretations." The memorandum instructed each agency conducting such an investigation to consult with the Attorney General to ascertain whether the agency's practices were fully in accord with the law. Subsequently, in September 1965, the Director of the FBI wrote the Attorney General and referred to the—

\* \* \* present atmosphere, brought about by the unrestrained and injudicious use of special investigative techniques by other agencies and departments, resulting in Congressional and public alarm and opposition to any activity which could in any way be termed an invasion of privacy. As a consequence, we have discontinued completely the use of microphones.

The Attorney General responded in part as follows:

The use of wiretaps and microphones involving trespass present more difficult problems because of the inadmissibility of any evidence obtained in court cases and because of current judicial and public attitude regarding their use. It is my understanding that such devices will not be used without my authorization, although in emergency circumstances they may be used subject to my later ratification. At this time I believe it desirable that all such techniques be confined to the gathering of intelligence in national security matters, and I will continue to approve all such requests in the future as I have in the past. I see no need to curtail any such activities in the national security field.

That was the Attorney General in 1965.

The CHAIRMAN. Is that still the policy?

Attorney General LEVI. That is not quite the policy which I will try to explain.

The CHAIRMAN. Fine.

Attorney General LEVI. The policy of the Department was stated publicly by the Solicitor General in a supplemental brief in the Supreme Court in *Black v. United States* in 1966. Speaking of the general delegation of authority by Attorneys General to the Director of the Bureau, the Solicitor General stated in his brief:

Present Departmental practice, adopted in July, 1965 in conformity with the policies declared by the President on June 30, 1965, for the entire Federal establishment, prohibits the use of such listening devices, as well as the interception of telephone and other wire communications, in all instances other than those involving the collection of intelligence affecting the national security. The specific authorization of the Attorney General must be obtained in each instance when this exception is invoked.

The Solicitor General made a similar statement in another brief filed that same term again emphasizing that the data would not be made available for prosecutorial purposes, and that the specific authorization of the Attorney General must be obtained in each instance when the national security is sought to be invoked.

In 1968, Congress passed the Omnibus Crime Control and Safe Streets Act. Title III of the act set up a detailed procedure for the interception of wire or oral communications. The procedure requires the issuance of a judicial warrant, prescribes the information to be set forth in the petition to the judge so that, among other things, he may find probable cause that a crime has been or is about to be committed. It requires notification to the parties subject to the intended surveillance within a period not more than 90 days after the application for an order of approval has been denied or after the termination of the period of the order or the period of the extension of the order. Upon a showing of good cause the judge may postpone the notification.

The act contains a saving clause to the effect that it does not limit the constitutional power of the President to take such measures as he deems necessary to protect the Nation against actual or potential attack or other hostile acts of a foreign power, to obtain foreign intelligence information deemed essential to the security of the United States, or to protect national security information against foreign intelligence activities. Then in a separate sentence the proviso goes on to say:

Nor shall anything contained in this chapter be deemed to limit the constitutional power of the President to take such measures as he deems necessary to protect the United States against the overthrow of the government by force or other unlawful means, or against any other clear and present danger to the structure or existence of the government.

Congress simply left presidential powers where it found them. Now I think a very responsible thing for a Congress to have done, I may say—

The CHAIRMAN. May I ask you what you meant by that?

Attorney General LEVI. I meant, in a matter of this importance, Congress should speak so that its intention is clear and if it meant to affirm this power, as I rather suspect that it did, there should be no ambiguity. But if it meant to pass an act that left a matter of this kind dangling in the air, I do not regard that as responsible.

Senator MATHIAS. Mr. Chairman, let me just say I support the Attorney General absolutely. When we asked about the overload in the courts, it would be much more effective if the Congress, instead of creating new judgeships, would simply write the laws more accurately and more precisely so that there would not have to be as many lawsuits or those we have to be so protracted. And I think the Attorney General has chided us in a way that is entirely justified. To this indictment I think the Congress has to plead guilty.

The CHAIRMAN. In principle I agree, although I think the effect of your proposal may greatly augment the rolls of the unemployed in this country.

Senator MATHIAS. Unemployed lawyers. We have acted as a legal employment bureau long enough, I think.

The CHAIRMAN. All right, Mr. Attorney General.

Attorney General LEVI. In the *Keith* case the Supreme Court held that in the field of internal security, if there was no foreign involvement, a judicial warrant was required by the fourth amendment. Fifteen months after the *Keith* case Attorney General Richardson, in a letter to Senator Fulbright, which was publicly released by the Department, stated:

In general, before I approve any new application for surveillance without a warrant, I must be convinced that it is necessary (1) to protect the nation against actual or potential attack or other hostile acts of a foreign power; (2) to obtain foreign intelligence information deemed essential to the security of the United States; or (3) to protect national security information against foreign intelligence activities.

I have read the debates and the reports of the Senate Judiciary Committee with respect to title III and, particularly, the proviso. It may be relevant to point out that Senator Philip Hart questioned and opposed the form of the proviso reserving presidential power. But I believe it is fair to say that his concern was primarily, perhaps exclusively, with the language which dealt with presidential power to take such measures as the President deemed necessary to protect the United States "against any other clear and present danger to the structure or existence of the Government."

I now come to the Department of Justice's present position on electronic surveillance conducted without a warrant. Under the standards and procedures established by the President, the personal approval of the Attorney General is required before any nonconsensual electronic surveillance may be instituted within the United States without a ju-

dicial warrant. All requests for surveillance must be made in writing by the Director of the Federal Bureau of Investigation and must set forth the relevant circumstances that justify the proposed surveillance; Both the agency and the Presidential appointee initiating the request must be identified. These requests come to the Attorney General after they have gone through review procedures within the Federal Bureau of Investigation. At my request, they are then reviewed in the Criminal Division of the Department. Before they come to the Attorney General, they are then examined by a special review group which I have established within the Office of the Attorney General. Each request, before authorization or denial, receives my personal attention. Requests are only authorized when the requested electronic surveillance is necessary to protect the Nation against actual or potential attack or other hostile acts of a foreign power; to obtain foreign intelligence deemed essential to the security of the Nation; to protect national security information against foreign intelligence activities; or to obtain information certified as necessary for the conduct of foreign affairs matters important to the national security of the United States.

In addition the subject of the electronic surveillance must be consciously assisting a foreign power or foreign-based political group, and there must be assurance that the minimum physical intrusion necessary to obtain the information sought will be used. As these criteria will show and as I will indicate at greater length later in discussing current guidelines the Department of Justice follows, our concern is with respect to foreign powers or their agents. In a public statement made last July 9, speaking of the warrantless surveillances then authorized by the Department, I said:

It can be said that there are no outstanding instances of warrantless wiretaps or electronic surveillance directed against American citizens and none will be authorized by me except in cases where the target of surveillance is an agent or collaborator of a foreign power.

This statement accurately reflects the situation today as well.

Having described in this fashion something of the history and conduct of the Department of Justice with respect to telephone wiretaps and microphone installations. I should like to remind the committee of a point with which I began, namely, that the factual situations to be imagined for a discussion such as this are not only of a sensitive but a changing nature. I do not have much to say about this except to recall some of the language used by General Allen in his testimony before this committee. The techniques of the NSA, he said, are of the most sensitive and fragile character. He described as the responsibility of the NSA the interception of international communication signals sent through the air. He said there had been a watch list, which among many other names, contained the names of U.S. citizens.

Senator Tower spoke of an awesome technology—a huge vacuum cleaner of communications—which had the potential for abuses. General Allen pointed out that "The United States, as part of its effort to produce foreign intelligence, has intercepted foreign communications to produce such foreign intelligence since the Revolutionary War." He said the mission of NSA is directed to foreign intelligence obtained from foreign electrical communications and also from other foreign signals, such as radar. Signals are intercepted by many techniques and processed, sorted, and analyzed by procedures which re-

ject inappropriate or unnecessary signals. He mentioned that the interception of communications, however it may occur, is conducted in such a manner as to minimize the unwanted messages. Nevertheless, according to his statement, many unwanted communications are potentially selected for further processing. He testified that subsequent processing, sorting, and selection for analysis are conducted in accordance with strict procedures to insure immediate and, wherever possible, automatic rejection of inappropriate messages. The analysis and reporting is accomplished only for those messages which meet specific conditions and requirements for foreign intelligence. The use of lists of words, including individual names, subjects, locations, et cetera, has long been one of the methods used to sort out information of foreign intelligence value from that which is not of interest.

General Allen mentioned a very interesting statute, 18 U.S.C. 952, to which I should like to call your particular attention. The statute makes it a crime for any one who by virtue of his employment by the United States obtains any official diplomatic code and willfully publishes or furnishes to another without authorization any such code or any other matter which was obtained while in the process of transmission between any foreign government and its diplomatic mission in the United States. I call this to your attention, because a certain indirection is characteristic of the development of law, whether by statute or not, in this area.

The CHAIRMAN. Can you explain what you mean by that last sentence? Are you suggesting that the law you have cited upon its face makes the activities of the NSA illegal?

Attorney General LEVI. I think that the law on its face seems to be a law to protect the actions of the NSA from having any transmission of messages intercepted go to unauthorized persons. The statute avoids by indirection saying that this is what the U.S. Government should do. It is assumed that it does it, and proceeds to find some way to give added potential.

The CHAIRMAN. That particular statute is specifically limited to codes between foreign governments and its diplomatic mission in the United States, is it not?

Attorney General LEVI. That is right.

As I say, it has a certain indirection.

The CHAIRMAN. Yes.

Attorney General LEVI. The committee will at once recognize that I have not attempted to summarize General Allen's testimony, but rather to recall it so that the extended dimensions of the variety of fact situations which we have to think about as we explore the coverage and direction of the fourth amendment is at least suggested.

Having attempted to provide something of a factual base for our discussion, I turn now to the fourth amendment. Let me say at once, however, that while the fourth amendment can be a most important guide to values and procedures, it does not mandate automatic solutions.

The history of the fourth amendment is very much the history of the American Revolution and this Nation's quest for independence. The amendment is the legacy of our early years and reflects values most cherished by the Founders. In a direct sense, it was a reaction to the general warrants and writs of assistance employed by the officers of

the British Crown to rummage and ransack colonists' homes as a means to enforce antismuggling and customs laws. General search warrants had been used for centuries in England against those accused of seditious libel and other offenses. These warrants, sometimes judicial, sometimes not, often general as to persons to be arrested, places to be searched, and things to be seized, were finally condemned by Lord Camden in 1765 in *Entick v. Carrington*, a decision later celebrated by the Supreme Court as a landmark of English liberty one of the permanent monuments of the British Constitution."

The case involved a general warrant, issued by Lord Halifax as Secretary of State, authorizing messengers to search for John Entick and to seize his private papers and books. Entick had written publications criticizing the Crown and was a supporter of John Wilkes, the famous author and editor of the "North Briton" whose own publications had prompted wholesale arrests, searches, and seizures. Entick sued for trespass and obtained a jury verdict in his favor. In upholding the verdict, Lord Camden observed that if the Government's power to break into and search homes were accepted, "the secret cabinets and bureaus of every subject in this kingdom would be thrown open to the search and inspection of a messenger, whenever the secretary of state shall see fit to charge, or even to suspect, a person to be the author, printer, or publisher of a seditious libel."

The practice of the general warrants, however, continued to be known in the colonies. The writ of assistance, an even more arbitrary and oppressive instrument than the general warrant, was also widely used by revenue officers to detect smuggled goods. Unlike a general warrant, the writ of assistance was virtually unlimited in duration and did not have to be returned to the court upon its execution. It broadly authorized indiscriminate searches and seizures against any person suspected by a customs officer of possessing prohibited or uncustomed goods.

The writs, sometimes judicial, sometimes not, were usually issued by colonial judges and vested Crown officers with unreviewed and unbounded discretion to break into homes, rifle drawers, and seize private papers. All officers and subjects of the Crown were further commanded to assist in the writ's execution. In 1761, James Otis eloquently denounced the writs as "the worst instrument of arbitrary power, the most destructive of English liberty, and the fundamental principles of law, that ever was found in an English law book," since they put "the liberty of every man in the hands of every petty officer." Otis' fiery oration later prompted John Adams to reflect that "then and there was the first scene of the first act of opposition to the arbitrary claims of Great Britain. Then and there the child Independence was born."

The words of the fourth amendment are mostly the product of James Madison. His original version appeared to be directed solely at the issuance of improper warrants. Revisions accomplished under circumstances that are still unclear transformed the amendment into two separate clauses. The change has influenced our understanding of the nature of the rights it protects. As embodied in our Constitution, the amendment reads:

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

Our understanding of the purposes underlying the fourth amendment has been an evolving one. It has been shaped by subsequent historical events, by the changing conditions of our modern technological society, and by the development of our own traditions, customs, and values. From the beginning, of course, there has been agreement that the amendment protects against practices such as those of the Crown officers under the notorious general warrants and writs of assistance. Above all, the amendment safeguards the people from unlimited, undue infringement by the Government on the security of persons and their property.

But our perceptions of the language and spirit of the amendment have gone beyond the historical wrongs the amendment was intended to prevent. The Supreme Court has served as the primary explicator of these evolving perceptions and has sought to articulate the values the amendment incorporates. I believe it is useful in our present endeavor to identify some of these perceived values.

First, broadly considered, the amendment speaks to the autonomy of the individual against society. It seeks to accord to each individual, albeit imperfectly, a measure of the confidentiality essential to the attainment of human dignity. It is a shield against indiscriminate exposure of an individual's private affairs to the world—an exposure which can destroy, since it places in jeopardy the spontaneity of thought and action on which so much depends. As Justice Brandeis observed in his dissent in the *Olmstead* case, in the fourth amendment the Founders "conferred, as against the Government, the right to be let alone—the most comprehensive of rights and the right most valued by civilized men." The amendment does not protect absolutely the privacy of an individual. The need for privacy, and the law's response to that need, go beyond the amendment. But the recognition of the value of individual autonomy remains close to the amendment's core.

A parallel value has been the amendment's special concern with intrusions when the purpose is to obtain evidence to incriminate the victim of the search. As the Supreme Court observed in *Boyd*, which involved an attempt to compel the production of an individual's private papers, at some point the fourth amendment's prohibition against unreasonable searches and seizures and the fifth amendment's prohibition against compulsory self-incrimination "run almost into each other." The intrusion on an individual's privacy has long been thought to be especially grave when the search is based on a desire to discover incriminating evidence. The desire to incriminate may be seen as only an aggravating circumstance of the search, but it has at times proven to be a decisive factor in determining its legality. Indeed, in *Boyd* the court declared broadly that "compelling the production of (a person's) private books and papers, to convict him of crime, or to forfeit his property, is contrary to the principles of a free government." The incriminating evidence point goes to the integrity of the criminal justice system. It does not necessarily settle the issue whether the overhearing can properly take place. It goes to the use and purpose of the information overheard.

An additional concern of the amendment has been the protection of freedom of thought, speech, and religion. The general warrants were used in England as a powerful instrument to suppress what was

regarded as seditious libel or nonconformity. So Justice Powell stated in *Keith* that "fourth amendment protections become the more necessary when the targets of official surveillance may be those suspected of unorthodoxy in their political beliefs."

Another concern embodied in the amendment may be found in its second clause dealing with the warrant requirement, even though the fourth amendment does not always require a warrant. The fear is that the law enforcement officer, if unchecked, may misuse his powers to harass those who hold unpopular or simply different views and to intrude capriciously upon the privacy of individuals. It is the recognition of the possibility for abuse, inherent whenever executive discretion is uncontrolled, that gives rise to the requirement of a warrant. That requirement constitutes an assurance that the judgment of a neutral and detached magistrate will come to bear before the intrusion is made and that the decision whether the privacy of the individual must yield to a greater need of society will not be left to the executive alone.

A final value reflected in the fourth amendment is revealed in its opening words: "The right of the people." Who are "the people" to whom the amendment refers? The Constitution begins with the phrase, "We the People of the United States." That phrase has the character of words of art, denoting the power from which the Constitution comes. It does suggest a special concern for the American citizen and for those who share the responsibilities of citizens. The fourth amendment guards the right of "the people" and it can be urged that it was not meant to apply to foreign nations, their agents and collaborators. Its application may at least take account of that difference.

The values outlined above have been embodied in the amendment from the beginning. But the importance accorded a particular value has varied during the course of our history. Some have been thought more important or more threatened than others at time. When several of the values coalesce, the need for protection has been regarded as greatest. When only one is involved, that need has been regarded as lessened. Moreover, the scope of the amendment itself has been altered over time. Words have been read by different justices and different courts to mean different things. The words of the amendment have not changed; we, as a people, and the world which envelops us, have changed.

An important example is what the amendment seeks to guard as "secure." The wording of the fourth amendment suggests a concern with tangible property. By its terms, the amendment protects the right of the people to be secure in their "persons, houses, papers and effects." The emphasis appears to be on the material possessions of a person, rather than on his privacy generally.

The CHAIRMAN. Why do you say that when the word "persons" comes first; "houses, papers and effects" comes after "persons?" It seems to me that the emphasis was on persons in the first instance, and material holdings afterward.

Attorney General Levi. I suspect one reason you think so, Mr. Chairman, is the fact that you are living today, but the emphasis on property and property rights, I think, was the way the amendment was previously looked at. There is an interesting exchange between Sir

Frederick Pollack and Justice Holmes on that very subject at the time of the *Olmstead* case.

In any event, this emphasis on property was the conclusion the court came to on the *Olmstead* case in 1928, holding that the intercept of telephone messages, if accomplished without a physical trespass, was outside the scope of the fourth amendment. Chief Justice Taft, writing for the court, reasoned that wiretapping did not involve a search or seizure; the amendment protected only tangible material "effects" and not intangibles such as oral conversations.

But, while the removal and carrying off of papers was a trespass of the most aggravated sort, inspection alone was not: "The eye," Lord Camden said, "cannot by the law of England be guilty of a trespass."

The CHAIRMAN. Did he really say that?

Attorney General LEVI. Yes; he did.

The movement of the law since *Olmstead* has been steadily from protection of property to the protection of privacy. In the *Goldman* case in 1942 the Court held that the use of a detectaphone placed against the wall of a room to overhear oral conversations in an adjoining office was not unlawful because no physical trespass was involved. The opinion's unstated assumption, however, appeared to be that a private oral conversation could be among the protected "effects" within the meaning of the fourth amendment. The *Silverman* case later eroded *Olmstead* substantially by holding that the amendment was violated by the interception of an oral conversation through the use of a spike mike driven into a party wall, penetrating the heating duct of the adjacent home. The Court stated that the question whether a trespass had occurred as a technical matter of property law was not controlling; the existence of an actual intrusion was sufficient.

The Court finally reached the opposite emphasis from its previous stress on property in 1967 in *Katz v. United States*. The Court declared that the fourth amendment "protects people, not places," against unreasonable searches and seizures; that oral conversations, although intangible, were entitled to be secure against the uninvited ear of a government officer, and that the interception of a telephone conversation, even if accomplished without a trespass, violated the privacy on which petitioner justifiably relied while using a telephone booth. Justice Harlan, in a concurring opinion, explained that to have a constitutionally protected right of privacy under *Katz* it was necessary that a person, first, "have exhibited an actual—subjective—expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'"

At first glance, *Katz* might be taken as a statement that the fourth amendment now protects all reasonable expectations of privacy—that the boundaries of the right of privacy are coterminous with those of the fourth amendment. But that assumption would be misleading. To begin with, the amendment still protects some interests that have very little, if anything, to do with privacy. Thus, the police may not, without warrant, seize an automobile parked on the owner's driveway even though they have reason to believe that the automobile was used in committing a crime. The interest protected by the fourth amendment in such a case is probably better defined in terms of property than privacy. Moreover, the *Katz* opinion itself cautioned that "the fourth amendment cannot be translated into a general constitutional 'right

to privacy.' " Some privacy interests are protected by remaining Constitutional guarantees. Others are protected by Federal statute, by the States, or not at all.

The CHAIRMAN. May I interrupt at this point to suggest that there is a vote in the Senate, a roll-call, which accounts for the fact that the Senators have had to leave. It looks as though the balance of your statement will require the remainder of the session this morning, so that I would suggest, if it is possible for you to do so, that we return upon the completion of your testimony, that we return this afternoon in order that Members then may have an opportunity, having heard parts of your statement and read the rest, to ask questions.

At 2 o'clock this afternoon, we will continue the questioning. I am not going to go to the vote. I am very much interested in the paper. I would like you to continue, please.

Attorney General LEVI. The point that I was making about *Katz* is twofold. First, under the Court's decisions, the fourth amendment does not protect every expectation of privacy, no matter how reasonable or actual that expectation may be. It does not protect, for example, against false friends' betrayals to the police of even the most private confidences. Second, the "reasonable expectation of privacy" standard; often said to be the test of *Katz*, is itself a conclusion. It represents a judgment that certain behavior should as a matter of law be protected against unrestrained governmental intrusion. That judgment, to be sure, rests in part on an assessment of the reasonableness of the expectation, that is, on an objective, factual estimation of a risk of intrusion under given circumstances, joined with an actual expectation of privacy by the person involved in a particular case. But it is plainly more than that, since it is also intermingled with a judgment as to how important it is to society that an expectation should be confirmed—a judgment based on a perception of our customs, traditions, and values as a free people.

The *Katz* decision itself illustrates the point. Was it really a "reasonable expectation" at the time of *Katz* for a person to believe that his telephone conversation in a public phone booth was private and not susceptible to interception by a microphone on the booth's outer wall? Almost 40 years earlier in *Olmstead*, the Court held such nontrespassory interceptions were permissible. *Goldman* reaffirmed that holding. So how could *Katz* reasonably expect the contrary? The answer, I think, is that the Court's decision in *Katz* turned ultimately on an assessment of the effect of permitting such unrestrained intrusions on the individual in his private and social life. The judgment was that a license for unlimited governmental intrusions upon every telephone would pose too great a danger to the spontaneity of human thought and behavior. Justice Harlan put the point this way: "The analysis must, in my view, transcend the search for subjective expectations or legal attribution of assumptions of risk. Our expectations, and the risks we assume, are in large part reflections of laws that translate into rules the customs and values of the past and present." A weighing of values is an inescapable part in the interpretation and growth of the fourth amendment. Expectations, and their reasonableness, vary according to circumstances. So will the need for an intrusion and its likely effect. These elements will define the boundaries of the interests which the amendment holds as "secure."

To identify the interests which are to be "secure," of course, only begins the inquiry. It is equally essential to identify the dangers from which those interests are to be secure. What constitutes an intrusion will depend on the scope of the protected interest. The early view that the fourth amendment protected only tangible property resulted in the rule that a physical trespass or taking was the measure of an intrusion. *Olmstead* rested on the fact that there had been no physical trespass into the defendant's home or office. It also held that the use of the sense of hearing to intercept a conversing did not constitute a search or seizure. *Katz*, by expanding the scope of the protected interests, necessarily altered our understanding of what constitutes an intrusion. Since intangibles such as oral conversations are now regarded as protected "effects," the overhearing of a conversation may constitute an intrusion apart from whether a physical trespass is involved. The nature of the search and seizure can be very important. An entry into a house to search its interior may be viewed as more serious than the overhearing of a certain type of conversation. The risk of abuse may loom larger in one case than the other. The factors that have come to be viewed as most important, however, are the purpose and effect of the intrusion. The Supreme Court has tended to focus not so much on what was physically done, but on why it was done and what the consequence is likely to be. What is seized, why it was seized, and what is done with what is seized are critical questions.

I stated earlier that a central concern of the fourth amendment was with intrusions to obtain evidence to incriminate the victim of the search. This concern has been reflected in Supreme Court decisions which have traditionally treated intrusions to gather incriminatory evidence differently from intrusions for neutral or benign purposes. In *Frank v. Maryland*, 359 U.S. 360 (1959), the appellant was fined for refusing to allow a housing inspector to enter his residence to determine whether it was maintained in compliance with the municipal housing code. Violation of the code would have led only to a direction to remove the violation. Only failure to comply with the direction would lead to a criminal sanction. The Court, held that such administrative searches could be conducted without warrant. Justice Frankfurter, writing for the Court, noted that the fourth amendment was a reaction to "ransacking by Crown officers of the homes of citizens in search of evidence of crime or of illegally imported goods." He observed that both *Entick* and *Boyd* were concerned with attempts to compel individuals to incriminate themselves in criminal cases and that "it was on the issue of the right to be secure from searches for evidence to be used in criminal prosecutions or for forfeitures that the great battle for fundamental liberty was fought." There was thus a great difference, the Justice said, between searches to seize evidence for criminal prosecutions and searches to detect the existence of municipal health code violations. Searches in this latter category, conducted "as an adjunct to a regulatory scheme for the general welfare of the community and not as a means of enforcing the criminal law, have antecedents deep in our history," and should not be subjected to the warrant requirement.

*Frank* was later overruled in 1967 in *Camara v. Municipal Court*, and a companion case, *See v. City of Seattle*. In *Camara*, appellant was, like *Frank*, charged with a criminal violation as a result of his

refusal to permit a municipal inspector to enter his apartment to investigate possible violations of the city's housing code. The Supreme Court rejected the *Frank* rationale that municipal fire, health, and housing inspections could be conducted without a warrant because the object of the intrusion was not to search for the fruits or instrumentalities of crime. Moreover, the Court noted that most regulatory laws such as fire, health, and housing codes were enforced by criminal processes, that refusal to permit entry to an inspector was often a criminal offense, and that the "self-protection" or "noncrimination" objective of the fourth amendment was therefore indeed involved.

But the doctrine of *Camara* proved to be limited. In 1971 in *Wyman v. James* the Court held that a "home visit" by a welfare caseworker, which entailed termination of benefits if the welfare recipient refused entry, was lawful despite the absence of a warrant. The Court relied on the importance of the public's interest in obtaining information about the recipient, the reasonableness of the measures taken to insure that the intrusion was limited to the extent practicable, and most importantly, the fact that the primary objective of the search was not to obtain evidence for a criminal investigation or prosecution. *Camara* and *Frank* were distinguished as involving criminal proceedings.

Perhaps what these cases mainly say is that the purpose of the intrusion, and the use to which what is seized is put, are more important from a constitutional standpoint than the physical act of intrusion itself. Where the purpose or effect is noncriminal, the search and seizure is perceived as less troublesome and there is a readiness to find reasonableness even in the absence of a judicial warrant. By contrast, where the purpose of the intrusion is to gather incriminatory evidence, and hence hostile, or when the consequence of the intrusion is the sanction of the criminal law, greater protections may be given.

The fourth amendment then, as it has always been interpreted, does not give absolute protection against Government intrusion. In the words of the amendment, the right guaranteed is security against unreasonable searches and seizures. As Justice White said in the *Camara* case, "there can be no ready test for determining reasonableness other than by balancing the need to search against the invasion which the search entails." Whether there has been a constitutionally prohibited invasion at all has come to depend less on an absolute dividing line between protected and unprotected areas, and more on an estimation of the individual security interests affected by the Government's actions. Those effects, in turn, may depend on the purpose for which the search is made, whether it is hostile, neutral, or benign in relation to the person whose interests are invaded, and also on the manner of the search.

By the same token, the Government's need to search, to invade individual privacy interests, is no longer measured exclusively, if indeed it ever was, by the traditional probable cause standard. The second clause of the amendment states, in part, that "no warrants shall issue but upon probable cause." The concept of probable cause has often been read to bear upon and in many cases to control the question of the reasonableness of searches, whether with or without warrant. The traditional formulation of the standard, as "reasonable grounds for believing that the law was being violated on the premises

to be searched" relates to the governmental interest in the prevention of criminal offenses, and to seizure of their instruments and fruits. This formulation once took content from the long-standing "mere evidence rule" that searches could not be undertaken "solely for the purpose of securing evidence to be used in a criminal or penal proceeding, but that they may be resorted to only when a primary right to such search and seizure may be found in the interest which the public may have in the property to be seized." The Government's interest in the intrusion, like the individual's interest in privacy, thus was defined in terms of property, and the right to search as well as to seize was limited to items, contraband and the fruits and instrumentalities of crime, in which the Government's interest was thought superior to the individual's. This notion, long eroded in practice, was expressly abandoned by the Court in 1967 in *Warden v. Hayden*. Thus, the detection of crime, the need to discover and use "mere evidence" may presently justify intrusion.

Moreover, as I have indicated, the Court has held that, in certain situations, something less than probable cause, in the traditional sense, may be sufficient ground for intrusion, if the degree of intrusion is limited strictly to the purposes for which it is made. In *Terry v. Ohio*, the Court held that a policeman, in order to protect himself and others nearby, may conduct a limited "pat down" search for weapons when he has reasonable grounds for believing that criminal conduct is taking place and that the person searched is armed and dangerous. Last term, in *United States v. Brignoni-Ponce*, the Court held that, if an officer has a "founded suspicion" that a car in a border areas contains illegal aliens, the officer may stop the car and ask the occupants to explain suspicious circumstances. The Court concluded that the important governmental interest involved, and the absence of practical alternatives, justified the minimal intrusion of a brief stop. In both *Terry* and *Brignoni*, the Court emphasized that a more drastic intrusion, a thorough search of the suspect or automobile, would require the justification of traditional probable cause. This point is reflected in the Court's decisions in *Almeida-Sanchez* and *Ortiz*, in which the Court held that, despite the interest in stemming illegal immigration, searches of automobiles either at fixed checkpoints or by roving patrols in places that are not the "functional equivalent" of borders could not be undertaken without probable cause.

Nonetheless, it is clear that the traditional probable cause standard is not the exclusive measure of the Government's interest. The kind and degree of interest required depend on the severity of the intrusion the Government seeks to make. The requirement of the probable cause standard itself may vary, as the Court made clear in *Camara*. That case, as you recall, concerned the nature of the probable cause requirement in the context of searches to identify housing code violations. The Court was persuaded that the only workable method of enforcement was periodic inspection of all structures, and concluded that because the search was not "personal in nature," and the invasion of privacy involved was limited, probable cause could be based on "appraisal of conditions in the area as a whole," rather than knowledge of the condition of particular buildings. "If a valid public interest justifies the intrusion contemplated," the Court stated, "then there is probable cause to issue a suitable restricted search warrant." In the *Keith*,

case, while holding that domestic national security surveillance, not involving the activities of foreign powers and their agents, was subject to the warrant requirement, the Court noted that the reasons for such domestic surveillance may differ from those justifying surveillances for ordinary crimes, and that domestic security surveillances often have to be long-range projects. For these reasons, a standard of probable cause to obtain a warrant different from the traditional standard would be justified: "Different standards may be compatible with the fourth amendment if they are reasonable both in relation to the legitimate need of Government for intelligence information and the protected rights of our citizens."

In brief, although at one time the "reasonableness" of a search may have been defined according to the traditional probable cause standard, the situation has now been reversed. Probable cause has come to depend on reasonableness, on the legitimate need of the Government and whether there is reason to believe that the precise intrusion sought, measured in terms of its effect on individual security, is necessary to satisfy it.

This point is critical in evaluating the reasonableness of searches or surveillances undertaken to protect national security. In some instances, the Government's interest may be, in part, to protect the Nation against specific actions of foreign powers or their agents, actions that are criminal offenses. In other instances, the interest may be to protect against the possibility of actions by foreign powers and their agents dangerous to national security, actions that may or may not be criminal. Or the interest may be solely to gather intelligence, in a variety of forms, in the hands of foreign agents and foreign powers, intelligence that may be essential to informed conduct of our Nation's foreign affairs. This last interest indeed may often be far more critical for the protection of the Nation than the detection of a particular criminal offense. The fourth amendment's standard of reasonableness as it has developed in the Court's decisions is sufficiently flexible to recognize this.

Just as the reasonableness standard of the amendment's first clause has taken content from the probable cause standard, so it has also come to incorporate the particularity requirement of the warrant clause, that warrants particularly describe "the place to be searched, and the persons or things to be seized." As one circuit court has written, although pointing out the remedy might not be very extensive "limitations on the fruit to be gathered tend to limit the quest itself." The Government's interest and purpose in undertaking the search defines its scope, and the societal importance of that purpose can be weighted against the effects of the intrusion on the individual. By precise definition of the objects of the search, the degree of intrusion can be minimized to that reasonably necessary to achieve the legitimate purpose. In this sense, the particularity requirement of the warrant clause is analogous to the minimization requirement of title III; that interceptions "be executed in such a way as to minimize the interception of communications not otherwise subject to interception" under the title.

But there is a distinct aspect to the particularity requirement, one that is often overlooked. An officer who has obtained a warrant based upon probable cause to search for particular items may in conducting

the search necessarily have to examine other items, some of which may constitute evidence of an entirely distinct crime. The normal rule under the plain view doctrine is that the officer may seize the latter incriminating items as well as those specifically identified in the warrant so long as the scope of the authorized search is not exceeded. The minimization rule responds to the concern about overly broad searches, and it requires an effort to limit what can be seized. It also may be an attempt to limit how it can be used. Indeed, this minimization concern may have been the original purpose of the "mere evidence" rule.

The concern about the use of what is seized may be most important for future actions. Until very recently, in fact, until the Court's 1971 decision in *Bivens*, the only sanction against an illegal search was that its fruits were inadmissible at any criminal trial of the person whose interest was invaded. So long as this was the only sanction, the courts, in judging reasonableness, did not really have to weigh any governmental interest other than that of detecting crimes. In practical effect, a search could only be "unreasonable" as a matter of law if an attempt was made to use its fruits for prosecution of a criminal offense. So long as the Government did not attempt such use the search could continue and the Government's interests, other than enforcing criminal laws, could be satisfied.

It may be said that this confuses rights and remedies; searches could be unreasonable even though no sanction followed. But I am not clear that this is theoretically so, and realistically it was not so. As I have noted earlier, the reasonableness of a search has depended, in major part, on the purpose for which it is undertaken and on whether that purpose, in relation to the person whom it affects, is hostile or benign. The search most hostile to an individual is one in preparation for his criminal prosecution. Exclusion of evidence from criminal trials may help assure that searches undertaken for ostensibly benign motives are not used as blinds for attempts to find criminal evidence, while permitting searches that are genuinely benign to continue. But there is a more general point. The effect of a government intrusion on individual security is a function, not only of the intrusion's nature and circumstances, but also of disclosure and of the use to which its product is put. Its effects are, perhaps greatest when it is employed or can be employed to impose criminal sanctions or to deter, by disclosure, the exercise of individual freedoms. In short, the use of the product seized bears upon the reasonableness of the search.

These observations have particular bearing on electronic surveillance. By the nature of the technology the "search" may necessarily be far broader than its legitimate objects. For example, a surveillance justified as the only means of obtaining valuable foreign intelligence may require the temporary overhearing of conversations containing no foreign intelligence whatever in order eventually to locate its object. To the extent that we can, by purely mechanical means, select out only that information that fits the purpose of the search, the intrusion is radically reduced. Indeed, in terms of effects on individual security, there would be no intrusion at all. But other steps may be appropriate. In this respect, I think we should recall the language and the practice for many years under former section 605 of the Communications Act. The act was violated, not by surveillance alone, but only by surveillance and disclosure in court or to the public. It may be

that if a critical government purpose justifies a surveillance, but because of technological limitations it is not possible to limit surveillance strictly to those persons as to whom alone surveillance is justified, one way of reducing the intrusion's effects is to limit strictly the revelation or disclosure or the use of its product. Minimization procedures can be very important.

In discussing the standard of reasonableness, I have necessarily described the evolving standards for issuing warrants and the standards governing their scope. But I have not yet discussed the warrant requirement itself, how it relates to the reasonableness standard and what purposes it was intended to serve. The relationship of the warrant requirement to the reasonableness standard was described by Justice Robert Jackson:

Any assumption that evidence sufficient to support a magistrate's disinterested determination to issue a search warrant will justify the officers in making a search without a warrant would reduce the amendment to a nullity and leave the people's homes secure only in the discretion of police officers.

The CHAIRMAN. That is Senator Mathias' previous point, that once Attorney General Jackson became Mr. Justice Jackson, he took a different view.

Attorney General LEVI. That may be, although I had not realized he had been a police officer. That is Justice Jackson.

The CHAIRMAN. He had been Attorney General.

Attorney General LEVI. I make a substantial distinction.

The CHAIRMAN. I recognize the distinction.

Attorney General LEVI. When the right of privacy must reasonably yield to the right of search is, as a rule, to be decided by a judicial officer, not by a policeman or government enforcement agent. That makes his point better.

The CHAIRMAN. Yes.

Attorney General LEVI. This view has not always been accepted by a majority of the Court; the Court's view of the relationship between the general reasonableness standard and the warrant requirement has shifted often and dramatically. But the view expressed by Justice Jackson is now quite clearly the prevailing position. The Court said in *Katz* that "searches conducted outside the judicial process, without prior approval by judge or magistrate, are *per se* unreasonable under the fourth amendment, subject only to a few specifically established and well-delineated exceptions." Such exceptions include those grounded in necessity, where exigencies of time and circumstances make resort to a magistrate practically impossible. These include, of course, the *Terry* stop and frisk and, to some degree, searches incident to arrest. But there are other exceptions, not always grounded in exigency, for example, some automobile searches, and at least some kinds of searches not conducted for purposes of enforcing criminal laws, such as the welfare visits of *Wyman v. James*. In short, the warrant requirement itself depends on the purpose and degree of intrusion. A footnote to the majority opinion in *Katz*, as well as Justice White's concurring opinion, left open the possibility that warrants may not be required for searches undertaken for national security purposes. And, of course, Justice Powell's opinion in *Keith*, while requiring warrants for domestic security surveillances, suggests that a different balance may be struck when the surveillance is undertaken against foreign powers and

their agents to gather intelligence information or to protect against foreign threats.

The purpose of the warrant requirement is to guard against overzealousness of government officials, who may tend to overestimate the basis and necessity of intrusion and to underestimate the impact of their efforts on individuals.

The historical judgment, which the fourth amendment accepts, is that unreviewed executive discretion may yield too readily to pressures to obtain incriminating evidence and overlook potential invasions of privacy and protected speech.

These purposes of the warrant requirement must be kept firmly in mind in analyzing the appropriateness of applying it to the foreign intelligence and security area.

The CHAIRMAN. Mr. Attorney General, we are now on final passage of a bill. Since you have been testifying for some time, I think you could probably take a break, take a 5-minute recess, take a drink of water, and I think it would be inappropriate as we examine the vagaries of the fourth amendment for me to miss final vote on the Sunshine bill permitting congressional committees to hold open hearings.

Attorney General LEVI. Without a warrant.

The CHAIRMAN. Without a warrant, right.

[A brief recess was taken.]

The CHAIRMAN. The hearing will please come back to order.

Mr. Attorney General, would you take up where you left off, please?

Attorney General LEVI. There is a real possibility that application of the warrant requirement, at least in the form of the normal criminal search warrant, the form adopted in title III, will endanger legitimate government interests. As I have indicated, title III sets up a detailed procedure for interception of wire or oral communications. It requires the procurement of a judicial warrant and prescribes the information to be set forth in the petition to the judge so that, among other things, he may find probable cause that a crime has been or is about to be committed. It requires notification to the parties subject to the surveillance within a period after it has taken place. The statute is clearly unsuited to protection of the vital national interests in continuing detection of the activities of foreign powers and their agents. A notice requirement, aside from other possible repercussions, could destroy the usefulness of intelligence sources and methods. The most critical surveillance in this area may have nothing whatever to do with detection of crime.

Apart from the problems presented by particular provisions of title III, the argument against application of the warrant requirement, even with an expanded probable cause standard, is that judges and magistrates may underestimate the importance of the Government's need, or that the information necessary to make the determination cannot be disclosed to a judge or magistrate without risk of its accidental revelation, a revelation that could work great harm to the Nation's security. What is often less likely to be noted is that a magistrate may be as prone to overestimate as to underestimate the force of the Government's need. Warrants necessarily are used *ex parte*; often decision must come quickly on the basis of information that must remain confidential. Applications to any one judge or magistrate would be only sporadic; no opinion could be published; this would limit the growth of judicially developed, reasonably uniform standards based,

in part, on the quality of the information sought and the knowledge of possible alternatives. Equally important, responsibility for the intrusion would have been diffused. It is possible that the actual number of searches or surveillances would increase if executive officials, rather than bearing responsibility themselves, can find shield behind a magistrate's judgment of reasonableness. On the other hand, whatever the practical effect of a warrant requirement may be, it would still serve the important purpose of assuring the public that searches are not conducted without the approval of a neutral magistrate who could prevent abuses of the technique.

In discussing the advisability of a warrant requirement, it may also be useful to distinguish among possible situations that arise in the national security area. Three situations, greatly simplified, come to mind. They differ from one another in the extent to which they are limited in time or in target. First, the search may be directed at a particular foreign agent to detect a specific anticipated activity, such as the purchase of a secret document. The activity which is to be detected ordinarily would constitute a crime. Second, the search may be more extended in time, even virtually continuous, but still would be directed at an identified foreign agent. The purpose of such a surveillance would be to monitor the agent's activities, determine the identities of persons whose access to classified information he might be exploiting, and determine the identity of other foreign agents with whom he may be in contact. Such a surveillance might also gather foreign intelligence information about the agent's own country, information that would be of positive intelligence value to the United States. Third, there may be virtually continuous surveillance which by its nature does not have specifically predetermined targets. Such a surveillance could be designed to gather foreign intelligence information essential to the security of the Nation.

The more limited in time and target a surveillance is, the more nearly analogous it appears to be with a traditional criminal search which involves a particular target location or individual at a specific time. Thus, the first situation I just described would in that respect be most amenable to some sort of warrant requirement, the second less so. The efficacy of a warrant requirement in the third situation would be minimal. If the third type of surveillance I described were submitted to prior judicial approval, that judicial decision would take the form of an ex parte declaration that the program of surveillance designed by the Government strikes a reasonable balance between the Government's need for the information and the protection of individuals' rights. Nevertheless, it may be that different kinds of warrants could be developed to cover the third situation. In his opinion in *Almeida-Sanchez*, Justice Powell suggested the possibility of area warrants, issued on the basis of the conditions in the area to be surveilled, to allow automobile searches in areas near America's borders. The law has not lost its inventiveness, and it might be possible to fashion new judicial approaches to the novel situations that come up in the area of foreign intelligence. I think it must be pointed out that for the development of such an extended, new kind of warrant, a statutory base might be required or at least appropriate. At the same time, in dealing with this area, it may be mistaken to focus on the warrant requirement alone to the exclusion of other, possibly more realistic, protections.

What, then, is the shape of the present law? To begin with, several statutes appear to recognize that the Government does intercept certain messages for foreign intelligence purposes and that this activity must be, and can be, carried out. Section 952 of title 18, which I mentioned earlier is one example; section 798 of the same title is another. In addition, title III's proviso, which I have quoted earlier, explicitly disclaimed any intent to limit the authority of the Executive to conduct electronic surveillance for national security and foreign intelligence purposes. In an apparent recognition that the power would be exercised, title III specifies the conditions under which information obtained through Presidentially authorized surveillance may be received into evidence. It seems clear, therefore, that in 1968 Congress was not prepared to come to a judgment that the Executive should discontinue its activities in this area, nor was it prepared to regulate how those activities were to be conducted. Yet it cannot be said that Congress has been entirely silent on this matter. Its express statutory references to the existence of the activity must be taken into account.

The case law, although unsatisfactory in some respects, has supported or left untouched the policy of the Executive in the foreign intelligence area whenever the issue has been squarely confronted. The Supreme Court's decision in the *Keith* case in 1972 concerned the legality of warrantless surveillance directed against a domestic organization with no connection to a foreign power and the Government's attempt to introduce the product of the surveillance as evidence in the criminal trial of a person charged with bombing a CIA office in Ann Arbor, Mich. In part because of the danger that uncontrolled discretion might result in use of electronic surveillance to deter domestic organizations from exercising first amendment rights, the Supreme Court held that in cases of internal security, when there is no foreign involvement, a judicial warrant is required. Speaking for the Court, Justice Powell emphasized that—

This case involves only the domestic aspects of national security. We have expressed no opinion as to the issues which may be involved with respect to activities of foreign powers or their agents.

As I observed in my remarks at the ABA convention the Supreme Court surely realized—

in view of the importance the Government has placed on the need for warrantless electronic surveillance that, after the holding in *Keith*, the Government would proceed with the procedures it had developed to conduct those surveillances not prohibited—that is, in the foreign intelligence area or, as Justice Powell said, "with respect to activities of foreign powers and their agents."

The CHAIRMAN. May I interrupt to say that Justice Powell's perception of the latent threat of unwarranted surveillance against domestic organizations in the name of national security is of great concern to me and to the members of this committee because nothing could be more intimidating on the right of individuals to express themselves and protest policies of the Government with which they disagree, than the belief that they are being watched and their conversations are being monitored by the Federal Government.

Attorney General LEVI. As I believe you know, Mr. Chairman, it has also been a great concern to me.

The CHAIRMAN. I am simply expressing approval of the Powell opinion and its importance, and I am certain it is being observed.

Attorney General LEVI. The two Federal court decisions after *Keith*—I am not sure, Mr. Chairman, if that is a question. If it were a question, the answer is yes.

The two Federal court decisions after *Keith* that have expressly addressed the problem have both held that the fourth amendment does not require a warrant for electronic surveillance instituted to obtain foreign intelligence. In the first, *United States v. Brown*, the defendant, an American citizen, was incidentally overheard as the result of a warrantless wiretap authorized by the Attorney General for foreign intelligence purposes. In upholding the legality of the surveillance, the Court of Appeals for the Fifth Circuit declared that on the basis of "the President's constitutional duty to act for the United States in the field of foreign affairs, and his inherent power to protect national security in the conduct of foreign affairs, the President may constitutionally authorize warrantless wiretaps for the purpose of gathering foreign intelligence." The court added that "restrictions on the President's power which are appropriate in cases of domestic security become inappropriate in the context of the international sphere."

In the *United States v. Butenko*, the Third Circuit reached the same conclusion—that the warrant requirement of the fourth amendment does not apply to electronic surveillance undertaken for foreign intelligence purposes. Although the surveillance in that case was directed at a foreign agent, the court held broadly that the warrantless surveillance would be lawful so long as the primary purpose was to obtain foreign intelligence information. The court stated that such surveillance would be reasonable without a warrant even though it might involve the overhearing of conversations of "alien officials and agents, and perhaps of American citizens." I should note that although the United States prevailed in the *Butenko* case, the Department acquiesced in the petitioner's application for *certiorari* in order to obtain the Supreme Court's ruling on the question. The Supreme Court denied review, however, and thus left the third circuit's decision undisturbed as the prevailing law.

THE CHAIRMAN. Do you know anywhere in the prevailing law that the term "foreign intelligence" is defined?

Attorney General LEVI. I am not sure I can answer that question. I think that the constant emphasis on foreign powers and their agents helps define. In a discussion of the diplomatic powers of the President, his position in terms of the Armed Forces and so on perhaps helps.

THE CHAIRMAN. We find it a very elusive term because it can be applied as justification for most anything and broadly defined can go far beyond the criteria that you just suggested. I know no place in the law that undertakes to define the term.

Attorney General LEVI. That, of course, is the problem with all the terms in this area. Also, a problem with the term "internal security," "domestic security," or "national security," because one might tend to baffle those terms to the point that they cover foreign intelligence, so that we have a problem.

Most recently, in *Zweibon v. Mitchell*, decided in June of this year, the District of Columbia circuit dealt with warrantless electronic surveillance directed against a domestic organization allegedly en-

gaged in activities affecting this country's relations with a foreign power. It dealt specifically with the Jewish Defense League and the allegation that it was involved with bombing of foreign diplomats of importance to the U.N. Judge Skelly Wright's opinion for four of the nine judges makes many statements questioning any national security exception to the warrant requirement. The court's actual holding made clear in Judge Wright's opinion was far narrower and, in fact, is consistent with holdings in *Brown* and *Butenko*. The court held only that "a warrant must be obtained before a wiretap is installed on a domestic organization that is neither the agent of nor acting in collaboration with a foreign power." This holding, I should add, was fully consistent with the Department of Justice's policy prior to the time of the *Zweibon* decision.

The CHAIRMAN. Is it also prevailing law?

Attorney General LEVI. I regard it as prevailing law.

The CHAIRMAN. Is there an appeal pending? Is it being taken to the Supreme Court?

Attorney General LEVI. My understanding is that the Department is not taking an appeal. I am not sure of the defendants.

Since the Department's policy is really in agreement with the holding, the only way for us to accept as lawyers representing others to take an appeal, would have been to say that the broad language of the court was an attempt to make an illicit extension of its holding and to try to appeal on that. I do not believe you would have gotten anyplace. I would like to have done it partly as a way of telling judges that they should take care what they say.

With these cases in mind, it is fair to say electronic surveillance conducted for foreign intelligence purposes, essential to the national security, is lawful under the fourth amendment, even in the absence of a warrant, at least where the subject of the surveillance is a foreign power or an agent or collaborator of a foreign power. Moreover, the opinions of two circuit courts stress the purpose for which the surveillance is undertaken, rather than the identity of the subject. This suggests that in their view such surveillance without a warrant is lawful so long as its purpose is to obtain foreign intelligence.

But the legality of the activity does not remove from the Executive or from Congress the responsibility to take steps, within their power, to seek an accommodation between the vital public and private interests involved. In our effort to seek such an accommodation, the Department has adopted standards and procedures designed to insure the reasonableness under the fourth amendment of electronic surveillance and to minimize to the extent practical the intrusion on individual interests. As I have stated, it is the Department's policy to authorize electronic surveillance for foreign intelligence purposes only when the subject is a foreign power or an agent of a foreign power. By the term "agent" I mean a conscious agent; the agency must be of a special kind and must relate to activities of great concern to the United States for foreign intelligence or counterintelligence reasons. In addition at present there is no warrantless electronic surveillance directed against any American citizen, and although it is conceivable that circumstances justifying such surveillance may arise in the future, I will not authorize the surveillance unless it is clear that the American citizen is an active, conscious agent or collaborator of a foreign power. In no event, of course, would I authorize any warrantless sur-

veillance against domestic persons or organizations such as those involved in the *Keith* case. Surveillance without a warrant will not be conducted for purposes of security against domestic or internal threats. It is our policy, moreover, to use the title III procedure whenever it is possible and appropriate to do so, although the statutory provisions regarding probable cause, notification, and prosecutive purpose make it unworkable in all foreign intelligence and many counter-intelligence cases.

The standards and procedures that the Department has established within the United States seek to insure that every request for surveillance receives thorough and impartial consideration before a decision is made whether to institute it. The process is elaborate and time consuming, but it is necessary if the public interest is to be served and individual rights safeguarded.

I have just been speaking about telephone wiretapping and microphone surveillances which are reviewed by the Attorney General. In the course of its investigation, the committee has become familiar with the more technologically sophisticated and complex electronic surveillance activities of other agencies. These surveillance activities present somewhat different legal questions. The communications conceivably might take place entirely outside the United States. That fact alone, of course, would not automatically remove the agencies' activities from scrutiny under the fourth amendment since at times even communications abroad may involve a legitimate privacy interest of American citizens. Other communications conceivably might be exclusively between foreign powers and their agents and involve no American terminal. In such a case, even though American citizens may be discussed, this may raise less significant, or perhaps no significant, questions under the fourth amendment. But the primary concern, I suppose, is whether reasonable minimization procedures are employed with respect to use and dissemination.

With respect to all electronic surveillance, whether conducted within the United States or abroad, it is essential that efforts be made to minimize as much as possible the extent of that intrusion. Much in this regard can be done by modern technology. Standards and procedures can be developed and effectively deployed to limit the scope of the intrusion and the use to which its product is put. Various mechanisms can provide a needed assurance to the American people that the activity is undertaken for legitimate foreign intelligence purposes, and not for political or other improper purposes. The procedures used should not be ones which by the indirection in fact target American citizens and resident aliens where these individuals would not themselves be appropriate targets. The proper minimization criteria can limit the activity to its justifiable and necessary scope.

**The CHAIRMAN.** This is one of the subjects I'm sure the committee will want to question you about this afternoon because we had so much evidence of watch list and even random openings of the mail without any particular criteria, and names of people that would appear to be wholly inappropriate for purposes of surveillance. These are the real life questions that are presented to this committee in terms of what the Government actually has been doing.

**Attorney General Levi.** I assume, Mr. Chairman, that the main thrust of the committee is to see what kind of legislation or better procedures can be developed and I've tried very hard speaking on those

subjects that I can speak on, and not speaking on those that I cannot, to try to lay that down before the committee as a base.

Another factor must be recognized. It is the importance of potential importance of the information to be secured. The activity may be undertaken to obtain information deemed necessary to protect the Nation against actual or potential attack or other hostile acts of a foreign power, to obtain foreign intelligence information deemed essential to the security of the United States, or to protect national security information against foreign intelligence activities.

Need is itself a matter of degree. It may be that the importance of some information is slight, but that may be impossible to gauge in advance; the significance of a single bit of information may become apparent only when joined to intelligence from other sources. In short, it is necessary to deal in probabilities. The importance of information gathered from foreign establishments and agents may be regarded generally as high—although even here may be wide variations. At the same time, the effect on individual liberty and security—at least of American citizens—caused by methods directed exclusively to foreign agents, particularly with minimization procedures, would be very slight.

There may be regulatory and institutional devices other than the warrant requirement that would better assure that intrusions for national security and foreign intelligence purposes reasonably balance the important needs of Government and of individual interests. In assessing possible approaches to this problem it may be useful to examine the practices of other Western democracies. For example, England, Canada, and West Germany each share our concern about the confidentiality of communications within their borders. Yet each recognizes the right of the Executive to intercept communications without a judicial warrant in cases involving suspected espionage, subversion or other national security intelligence matters.

In Canada and West Germany, which have statutes analogous to title III, the Executive in national security cases is exempt by statute from the requirement that judicial warrants be obtained to authorize surveillance of communications. In England, where judicial warrants are not required to authorize surveillance of communications in criminal investigations, the relevant statutes recognize an inherent authority in the Executive to authorize such surveillance in national security cases. In each case, this authority is deemed to cover interception of mail and telegrams, as well as telephone conversations.

In all three countries, requests for national security surveillance may be made by the nation's intelligence agencies. In each, a Cabinet member is authorized to grant the request. In England and West Germany, however, interception of communications is intended to be a last resort, used only when the information being sought is likely to be unobtainable by any other means. It is interesting to note, however, that both Canada and West Germany do require the Executive to report periodically to the legislature on its national security surveillance activities. In Canada, the Solicitor General files an annual report with the Parliament setting forth the number of national security surveillances initiated, their average length, a general description of the methods of interception or seizure used, and an assessment of their utility.

It may be that we can draw on these practices of other Western democracies, with appropriate adjustments to fit our system of separation of powers. The procedures and standards that should govern the use of electronic methods of obtaining foreign intelligence and of guarding against foreign threats are matters of public policy and values. They are of critical concern to the executive branch and to the Congress, as well as to the courts. The fourth amendment itself is a reflection of public policy and values—an evolving accommodation between governmental needs and the necessity of protecting individual security and rights. General public understanding of these problems is of paramount importance, to assure that neither the Executive, nor the Congress, nor the courts risk discounting the vital interests on both sides.

The problems are not simple. Evolving solutions probably will and should come—as they have in the past—from a combination of legislation, court decisions, and executive actions. The law in this area, as Lord Devlin once described the law of search in England, “is haphazard and ill-defined.” It recognizes the existence and the necessity of the Executive’s power. But the executive and the legislative are, as Lord Devlin also said, “expected to act reasonably.” The future course of the law will depend on whether we can meet that obligation.

**THE CHAIRMAN.** Indeed, it will, Mr. Attorney General, and I want to thank you for this very learned dissertation on the fourth amendment. I think that it will prompt a number of questions from the committee this afternoon. It is 12:30 now, and I had hoped that we might adjourn until 2 this afternoon.

**Senator Mathias?**

**Senator MATHIAS.** Mr. Chairman. I comply with the instruction of the Chair to withhold questions for the moment, but I was one of those urging the invitation of the Attorney General to the session because I anticipated a thorough and scholarly discussion of the subject. I think that the Attorney General has fully met all of our expectations, and this will be an important document on this whole subject, both among those who will cite it for support and those who will wish to argue against it. But I think that it is obviously an important document and I look forward to the dialog this afternoon.

**THE CHAIRMAN.** I think it goes further on the subject than any other previous statement of the Government from any source. Therefore, the committee appreciates the time and effort that you have given to it and we look forward to a chance to question this afternoon.

If there are no further comments, the hearing stands adjourned until 2 this afternoon.

[Whereupon, at 12:30 p.m., the hearing adjourned, to reconvene at 2 p.m. of the same day.]

#### AFTERNOON SESSION

**The CHAIRMAN.** The hearing will please come to order.

**Mr. Attorney General,** in your statement this morning, you testified:

I now come to the Department of Justice’s present position on electronic surveillance conducted without a warrant. Under the standards and procedures established by the President, the personal approval of the Attorney General is required before any nonconsensual electronic surveillance may be instituted within the United States without a judicial warrant.

Do you mean by that statement that your approval is required before any one may be bugged or wiretapped without a warrant as long as the target is within the United States? Is that correct?

Attorney General LEVI. Well, I really cannot quite mean that, because—I guess I can. I was going to say that title III, which of course has a warrant provision, permits States to do wiretapping, but I suppose that I do mean that without a judicial warrant, that is—

The CHAIRMAN. The existing practice?

Attorney General LEVI. The standard procedure established by the President.

The CHAIRMAN. Yes. Since it is a procedure established by the President, it could be changed at any time by the President.

Attorney General LEVI. I assume so.

The CHAIRMAN. What about electronic surveillance of messages that have one terminal outside the United States? Is your permission required before an unwarranted interception of such messages may take place?

Attorney General LEVI. Well, my belief is, if it is a surveillance which there is a base in the United States and a communication from the United States, which is what we would ordinarily think of as being covered, I think the Attorney General's approval would be required.

The CHAIRMAN. What about the messages that NSA snatches out of the air? They do not require your approval, do they?

Attorney General LEVI. You are now asking me about the NSA procedures.

The CHAIRMAN. I'm only asking you whether they require your approval.

Attorney General LEVI. I have only started to answer.

The CHAIRMAN. I see.

Attorney General LEVI. The first part of the answer is, I want to make this clear that I do not really know what the NSA procedures are. And I think that is an important point. I do not think that a briefing in which an Attorney General or some other kind of a lawyer is given a certain amount of information which adheres, means that the result of that is that the Attorney General knows what the procedures are. And at this time I would have to say that I do not know what the procedures are. I do not know what the possibilities are. I do not know enough about the minimization possibilities. The position on that is, we have asked that we be fully informed, that we be fully informed as to the leeways, the possible procedures, the possible minimization procedures, and the President has directed the NSA to provide that information to the Department of Justice, to the Attorney General, so that we can make some kind of a determination on it.

The CHAIRMAN. Until you have that information, you really do not have the foggiest idea of whether what they are doing is legal or illegal, constitutional or unconstitutional?

Attorney General LEVI. I would be glad to accept the protective shape of that proposed answer. I suppose I have a foggy idea.

The CHAIRMAN. You do not—

Attorney General LEVI. I do not think I should be in a position of making a determination about it until, for various reasons possibly, but not until I really know what it is and I have told you many times that I do not know what it is. We have requested that we be given a

full account, which is probably not too easy to give. We have requested that procedures be outlined. More important, that the possible protective procedures be outlined and the President has specifically directed them to give them to us.

The CHAIRMAN. These practices have been going on for a long time. Hundreds of thousands of American citizens have had their messages intercepted by the Government, analyzed, disseminated to various agencies of the Government. Do you not think that it is awfully late for the Attorney General to be inquiring about the procedures in order to determine their constitutionality? I commend you for doing it; this question is not meant to be critical of you, but looking back over the years that these practices have gone on, is it not a very late date that we should now be seriously inquiring into their constitutionality at the Justice Department?

Attorney General LEVI. One first has to remember that the law has changed, that some of those practices—I do not know which ones about the NSA you are referring to—began a long time ago, so as a matter of fact, I cannot say that other Attorneys General might not have, years ago, inquired into it. So I do not know how to answer that, except to say that I have not been around that long as Attorney General.

If you go back to 1947, 1949, you really had a different shape to it all, and one would have to look at it in those terms.

The CHAIRMAN. If I understood your testimony this morning correctly, you said that the President has the power to wiretap an American citizen without a warrant if he is an agent or a collaborator of a foreign power. This would be one of those cases where you, as the agent of the President, would approve of a wiretap without a judicial warrant. That is correct, is it not?

Attorney General LEVI. It is correct, although I never—I hope, I do not think that I said that that was all that we would look for.

The CHAIRMAN. Oh, no, I was just taking one example. You laid out the criteria. I think there were two or three things you would look for. But one was an agent or collaborator of a foreign power. I do not think that any of us would quarrel with a wiretap on a foreign agent as falling within the counterintelligence operations of the Government, and having to do with both foreign intelligence and national security.

What I am interested in is how you would view a foreign agent or collaborator. For example, what is a collaborator? Suppose you have young people who were protesting the war, for example, as so many did, and some of them met with certain foreign government officials. Would they then be regarded as collaborators? How does this term apply?

Attorney General LEVI. I think—I will answer directly—I do not want one to think that I am evading the question, but then I want to go on to say something more.

I would not think that that would make a person a collaborator. You have not given all the facts. You could turn it around and say, one cannot say that one is a collaborator because one is, at the same time, taking part in unpopular political causes. One has to look very carefully at what the kind of evidence is, and that really points to the procedure, which it seems to me in any constructive solution of this

kind of problem, one has to look to see what procedures are followed and what kind of evidence has to be weighed.

I am sure that there is really no absolutely automatic way of doing that. One of the strong arguments that is so frequently made for warrantless surveillance is that it is necessary to use it in order to determine whether someone is an agent or a conscious agent. That, of course, is certainly what we have tried to do is make sure that the evidence is better than that.

The CHAIRMAN. Of course, the difficulty is that judgment in a case of this kind, and I would suppose necessarily so, is made by interested parties, so to speak. The Attorney General is a member of the executive branch as an agent of the President. Unlike the ordinary law enforcement case, there is never a necessity to present the reasons that give probable cause to believe that a crime has been performed to some independent tribunal.

Therefore, the procedures and the criteria become very important. Just to press this, because I can think of other examples, I remember the case of Joseph Kraft, a distinguished columnist, meeting with certain foreign agents of a certain foreign government in Paris during the Vietnam war. In your view, he was presumably looking for news, looking for their viewpoints. Would that, in any sense, in your view, make him a collaborator and justify a wiretap?

Attorney General LEVI. Certainly not. I hope I have not said anything that suggests that.

The CHAIRMAN. I do not believe you have. I am just trying to clarify the boundaries by my questions.

Attorney General LEVI. Let me make the point, since we are talking about the foreign legislation remedies you take. If one had a statute, one of the things that I suppose that a judge might have to make some kind of finding on is whether there is evidence sufficient to establish the conscious collaboration of agents.

There is a problem there, because one would know that through the most secret sources, and disclosure might expose someone to assassination. It is the kind of thing which I suppose a judge could make a finding on. As far as the Attorney General's position is concerned, I think that the Attorney General probably feels that his position is one of protecting the laws of the United States, protecting the President. He is probably more vigilant on that account. I assure you that it is much easier for me to sign the title III than it is to handle these cases.

The CHAIRMAN. You have been, I think it is fair to say, a vigilant Attorney General, but that has not always been the case. We have had some Attorneys General who have paid very little heed to the law, and did pretty much as the President wanted them to do. So, unless we have some statutory guidelines, I think that it is very dangerous just to leave it to the Attorney General to decide, knowing that the office changes, and Presidents change. Do you think that there is any way that we could write into law certain statutory guidelines which would determine when warrantless surveillance would be permissible, what test must be met?

Attorney General LEVI. I would hope so. Other countries have been able to do it, and I would hope that this one could, although I am not absolutely confident, as I say, it would have to be the reason I

pointed out this morning. This is an area where people proceed frequently by statutes through indirection, in part, because of the nature of the problem. But I, myself, would hope that it would be possible to have a statute.

The CHAIRMAN. If this committee should decide that among its recommendations we should include a recommended statute that would govern warrantless surveillance in the general field of foreign intelligence and national security, would you be prepared, as Attorney General, to assist the committee in designing such a statute?

Attorney General LEVI. Of course. The more interesting question is whether the committee, since it has more power, would be willing to assist me.

The CHAIRMAN. The power of the committee in this case is merely that of recommending. The actual action upon any recommendations would have to go to the appropriate legislative committees of the Senate. But in any case, I should think that our collaboration may be fruitful, and I welcome it.

The other aspect of this case—there are many aspects of the case that are troubling me. Because other Senators are here now, I do not want to monopolize the time, but I would like to ask you just a question or two on another term that is constantly coming into use, the term "foreign intelligence." Here we have an agency, the NSA, which has no statutory base, by creation of an Executive order. Its scope of authority rests on certain executive directives that give it a general mission of obtaining foreign intelligence.

Now, as I suggested earlier, foreign intelligence has never been defined by statute, and I suppose that we could all agree that certain kinds of information would clearly be foreign intelligence. But we look at the NSA and we find that they are collecting all kinds of data on economic intelligence; that now falls in what we now call foreign intelligence, having to do with transfer of funds, business investments, the movement of capital.

Suppose that an American company was making a decision with respect to an investment in some foreign land, was interested in keeping that decision secret for business reasons, competitive reasons. Is that a case that would fall within the net of foreign intelligence, thus entitling the government to obtain that kind of information without a warrant, because it is generically a part of what we have come to call foreign intelligence? How do we grapple with this?

Attorney General LEVI. I think the way you have to grapple with it, Mr. Chairman, is not just to belabor the point of what the definition of foreign intelligence means, because, as you pointed out, it can include an enormous variety. It can include, for example, all kinds of economic information. And I am quite sure that professional intelligence people would think that a very wide net might be appropriate because small items of information all by themselves may not mean anything, as I said in my statement, but added to something else, they mean something. So you might have a very broad definition of foreign intelligence within that a very broad notion of important economic information, but certainly the inquiry does not stop there. One has to say, well, how did they get it? What is the target of the surveillance? Is it being obtained through the targeting of an official foreign unit, or is it targeted in such a way as to pick up American firms or Americans who are discussing these problems?

As I tried to say this morning, it seems to me that the fourth amendment coverage will depend to a considerable extent on the limitations one can impose. It is one thing, I think—although this is a very difficult field—for an American company to be discussing something with a foreign official establishment, and quite another thing when it is discussing it with some kind of a foreign concern. So that it is one thing where the information is picked up because the targeting is on the foreign governmental unit, or whatever it is, official unit, whatever it is, and quite another thing where the targeting, in fact, is on the American firm. A great deal will depend on how one—maybe one can mechanically, to a considerable extent, minimize that. When one gets to that point, one has to find out how one can go any further.

The CHAIRMAN. This committee knows that the NSA is one gigantic set of earphones and all kinds of requests are coming in as to what to listen to in the world, and the agencies themselves determine—I do not suppose that the President enters into it, clearly the Attorney General does not enter into it, no department of the government that is supposed to look out for the laws and the Constitution enters into it. We know some of the things they have done; some are laudable in terms of the ultimate objective, for example, drug traffic. That is a good thing to learn about. We are trying to enforce laws in this country, and information that you can get by listening in on telephone conversations—

Attorney General LEVI. Of American citizens abroad?

The CHAIRMAN. American citizens at one end of the terminal, and possibly an American citizen on the other, or a foreign citizen on the other; they listen to all the telephone conversations and extract ones relating to drugs. That is a laudable purpose, but is that foreign intelligence?

Attorney General LEVI. It may be foreign.

The CHAIRMAN. Or is that law enforcement?

Attorney General LEVI. It may be foreign intelligence, but as you stated quite broadly, and you stated quite broadly a number of possible situations. Some of them I would regard as unconstitutional. At that point the word—I cannot imagine the word intelligence is to be defined in such a way as to permit unconstitutional behavior.

The CHAIRMAN. Right. That is terribly important to say because very seldom can you get anybody, when you get into this field of national security, to say that it is subject to the Constitution. It is much more frequent for them to say in this area the Constitution is an archaic document of the 18th century, and we have to be practical about these things. I am not saying you suggested that, but I am happy for you to say that even in questions relating to foreign intelligence and national security, the Constitution and its guarantees remain applicable.

Attorney General LEVI. Mr. Chairman, there are arguments—I must say that I tried in the paper I gave this morning—in fact, Senator Mathias hurt my feelings by complimenting me. I was really trying to be quite neutral. I was really not making an argument on one side or the other. One argument that I did not include which is sometimes made is that if matters are picked up out of the air, so to speak, as waves of some kind go across the ocean, that there is no reason for people to assume that the conversations are private and therefore the

fourth amendment does not apply. I do not make that argument because I do not like it, I guess, and because I think it goes too far. I guess I say that only to say again that this is a very difficult field, and the procedures which are devised and the protections that are devised are terribly complicated.

**Senator MATHIAS.** If the chairman would yield, I do not think the Attorney General's feelings should be hurt by what I said because I believe I did indicate that there were those that might take this document and raise it as their banner and march off in one direction. There would be others who would take this document and raise it as their banner and march in the other.

**Attorney General LEVI.** I hoped that is what you were going to say, and I am delighted that you said it.

**The CHAIRMAN.** There is another example that the committee spent a week looking into, which was 20 years of opening the mail, conducted by the CIA in this case, and it developed in the course of the inquiry that some of this mail was opened because it was clearly foreign government mail.<sup>1</sup> Other mail was opened because various agencies had furnished the CIA with names of American citizens that they wanted watched. If a letter were coming to that citizen or were being sent by that citizen to a foreign address, that mail was opened. Other evidence showed that letters were also opened just at random, random selection to read and photograph and then to distribute to various agencies. Over the years, a quarter of a million letters were opened and photographed in this way. Do you think that that practice, which I think is a fair statement of the range of evidence that we received, conforms with the protections that are supposed to be conferred by the fourth amendment?

**Attorney General LEVI.** In one statement you mentioned, as I am sure you recognize, many different examples. You might have a letter which for some reason or another you get a warrant to open, and of course, that can be done. You might have letters written by or addressed to particular persons who might or might not be American citizens where you would have good reason to think that they were conscious collaborators, in a meaningful sense, of a foreign government. Then you would have the problem of where does the authorization to proceed under Presidential power, if that is what we are discussing, come from. And I think that one would have to look for the authorization.

Now, you are in an area where there is a criminal investigation by the Department, and I really should not say very much. I do want to say that if one goes back early enough in the forties Director Hoover had a particular position, I think, if I remember correctly, as censor of the mails, appointed by the President for that purpose. So that it does become a matter of some question as to authorization.

**The CHAIRMAN.** We have looked into the law and we cannot find any authorization for opening the mails. We find laws and court decisions against it. Certainly random opening of the mail could not possibly be reconciled with the fourth amendment.

**Attorney General LEVI.** I did not say that.

**The CHAIRMAN.** Could it?

---

<sup>1</sup> See Senate select committee hearings, vol. 4, Mail Opening.

Attorney General LEVI. I should not think the random opening could. Certainly in circumstances, I cannot imagine what circumstances to imagine, I suppose random mail from a particular source would no longer be random; so I do not know how to comment on that.

But I would like to go back to the authorization point because I think that what you have said suggests that there cannot be Presidential authorization for it. I have to say that I am not at all sure but I think that there could be a Presidential authorization under very limited circumstances. Then the question would be, would it have to be in writing. I do not know whether it has to be in writing or not. How does one know whether the authorization was given, is it believable, and so on and so on.

The CHAIRMAN. None of these procedures seem to exist in this area. It is part of the work of this committee to try to get them developed and established.

Attorney General LEVI. That is right. I hope the activities to which you are referring do not exist either.

The CHAIRMAN. At the moment, the particular mail opening operation has come to a halt, and since this investigation started, some of the NSA activities have come to a halt, but we would like to see some laws that would keep it that way.

Senator Huddleston.

Senator HUDDLESTON. Thank you, Mr. Chairman.

Attorney General Levi, I appreciate the detail and scholarly dissertation that you have given to this committee on this general subject. I did not hear all of it, but I did have an opportunity to read it. I am one of the few members of this committee that is not an attorney, which I am sure is apparent when I pose questions relating to legal problems. I am wondering, though, after reading your statement whether or not I might be qualified at least to apply for a license to practice law.

Attorney General LEVI. You mean the statement is so inferior that anybody else could do it, too.

Senator HUDDLESTON. If I learned all the knowledge there, I might have something to go along with my honorary doctorate degree of law.

Mr. Attorney General, there have been several court cases, one going back as far as 1928 in *Olstead v. United States* in which the majority held that wire tapping did not constitute a trespass over constitutional rights. Justice Brandeis in a dissent that said, "the progress of science in furnishing Government with the means of espionage is not likely to stop wiretapping. Ways may some day be developed by which the Government, without removal of papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to the jury the most intimate occurrences of a home." In a later case, 1963, *Lopez v. United States*, the effect of technology on the fourth amendment guarantees was again alluded to by the Court through Justice Brennan. He said that "this Court has by and large steadfastly held the fourth amendment against the physical intrusion of a person's home and property by law enforcement officers, but our course of decisions, it now seems, have been outflanked by the technological advances of the recent past." I am just wondering whether you think that the Court's present posture with regard to the fourth amendment has been outflanked by the technology that is now available.

Attorney General LEVI. No; I do not. I think, in fact, what the Court is doing is a little bit like what the Congress is doing, or has done, That is to say, that it knows that technological advances are occurring. It knows that many of these devices can be extremely important for good in the sense that they are essential to the security of the country, or for evil if they are misused. And it is difficult then for the Court, and I think for the Congress, to try to solve the whole problem at once.

I do not believe that the legal system, even though lawyers like sometimes to think it does, I do not think the legal system would say all of these efforts must be banned, period. I think that that is just much too simple. Therefore it is a complicated problem that has to be approached. I myself think it has been approached too piecemeal, I have constantly said that one can put the pieces together.

Senator HUDDLESTON. Are you saying that rather than attempt to legislate the kind of restrictions that would cover all of these possible situations, that we are going to have to rely on court interpretations of each case as we go along?

Attorney General LEVI. You will have court interpretations. And there will have to be procedures, because one cannot really be sure of what new developments will occur. One can build in reporting procedures, one can build in a variety of kinds of procedures to try to handle that.

Senator HUDDLESTON. In your statement you list four purposes of electronic surveillance. The first three come from language of Congress in the 1968 act, so-called conceptions of national security. The fourth one is new, which says "to obtain information certified as necessary for the conduct of foreign affairs matters important to the national security of the United States." Who certifies this?

Attorney General LEVI. As it says, it would have to be an appropriate Presidential appointee.

Senator HUDDLESTON. It may be somebody he may designate, Secretary of State, Director of Central Intelligence.

Attorney General LEVI. It would have to be a Presidential appointee.

Senator HUDDLESTON. In effect, on behalf of the President of the United States.

Attorney General LEVI. I am not sure it would just be that. I think that also speaks to the level of the responsibility that that President has and the appropriateness for him to give that kind of a certificate.

Senator HUDDLESTON. How does that reason differ from the second purpose that you have listed, which was to obtain foreign intelligence deemed essential to the security of the Nation?

Attorney General LEVI. It is an excellent question coming from a nonlawyer, and I interpret the two of them as the same. That has not always been a welcome interpretation.

Senator HUDDLESTON. It seems to me that the latter one would be a little broader.

Attorney General LEVI. I do not interpret it as broader. I interpret it as an attempt to say what foreign intelligence deemed essential to the security of the Nation might mean when it comes to the conduct of foreign affairs, but my flat answer is that the way I have interpreted that is to require that it be deemed essential.

Senator HUDDLESTON. In order for it to be important it has to be essential.

Attorney General LEVI. This is an area where, if you are going to have legislation or procedures, you will find that words of that kind are always used. That is true in the Canadian legislation. It is just generally true.

Senator HUDDLESTON. Another area that is almost foreign to me, as I understand the fourth amendment, it sets out very specifically that warrants should be obtained for instrusion, for search and seizure. It says, at least to me, that these warrants must be very specific, first of all, in the place which is going to be searched; second, in things that are to be seized. How can that be applied to a situation where, while the general purpose may be acceptable—that of security, that of maybe discovering a violation of law—the system is such that it is bound to bring in a lot of extraneous information. It is almost as though you had a warrant to search an apartment for drugs and you also walked out with the dining room table, because a lot of information that is picked up in conversations necessarily does not have anything at all to do with the original purpose.

Attorney General LEVI. If it were a notorious dining room table stolen from the White House and the person who went in for drugs could not help but notice it was there, I suppose it might be within the authority to take it.

Senator HUDDLESTON. I understand if it is a clear observation that there is something illegal about the dining room table, I would take it, too, maybe. In the case of picking up conversations, this is not the case. That is the first part of my question: How in the world can you prescribe the activity to the extent that you would eliminate in the first place getting this information which is a violation of privacy; more importantly, though, is the use of it?

In some of our inquiry there have been at least indications that some agencies have used information for the purpose of either embarrassing or discrediting individuals, although the specific information that they used, gathered from wiretaps, had no relationship at all to a crime or to the purpose that the wiretap was placed there. How do you keep that information from being used in such a way as to be detrimental to the citizen and when it is not related to the original purpose of the surveillance?

Attorney General LEVI. Senator, I really do not know how to answer that one. What you can do is to try to legislatively ban all operations. That, of course, would be an expression of the opinion of the Congress. It would raise a question whether it was Presidential power to continue it anyway, that you could attempt to ban it. I suppose the President could ban it.

Somehow or another that does not seem to me to be a constructive way to approach that kind of a problem because the fourth amendment was not originally conceived of as applying to these kinds of mechanisms anyway. The fourth amendment has shown, by so many other provisions in the Constitution, which is one reason why the Constitution works, that it can both carry important values and have a flexibility and yet have a real meaning of protection. The problem that you are asking me is; of course, the central problem referring to things like, again, the NSA operation which I think you are describing, but I am not sure.

Senator HUDDLESTON. That is true, except you have two parts of it because the NSA is just a collector, and it supplies the information to its so-called customers. They do not know what the customers do with it. The customers might use it in a way entirely different from what had been anticipated.

Attorney General LEVI. It is possible to devise procedures which undoubtedly are not perfect, designed to minimize it. What one has to do is see how far one can go in that, and then take a look at it and see whether the achievement is sufficient. That is one of the reasons that the President asked that these procedures be shown to us. That is the reason that we asked for the description, to see what procedures would be possible. I think the procedures can work at both ends, procedures as to what is picked up; you have to have procedures as to what use is made of it and where it goes.

Senator HUDDLESTON. Another elementary statement: Today under the present interpretation of laws if an individual found out that he had been maligned, damaged, or slandered by use of information that had been gathered in what started out as a legitimate surveillance, what recourse would he have? Could he sue anybody?

Attorney General LEVI. Again, I really do not know how to answer that question. You are asking me what is the relationship between surveillance which may have been proper, or may have been improper and the law of slander—it may be libel in the kind of case you describe. I just have to say I do not know the answer to that question. If I did know it, I would have to remind myself that the Department of Justice is defending a great many defendants in present cases where there are all kinds of lawsuits filed around the country. I do not think I should be making proclamations.

Senator HUDDLESTON. Also in your statement, you say there are appropriate and adequate standards for a person being wiretapped or bugged. The question is, these are your standards. Can they bind any successor of yours, or are they standards that are just constitutionally required by the fourth amendment?

Attorney General LEVI. Well, it is my view—two answers to that. In the first place, the only authority that I have in this area comes from the President, so that a good deal of what is decided is the authorization which is limited in that way by the President. I cannot authorize anything that goes beyond that. My interpretation of it is based on what I regard as the constitutional requirements which I think in this area respond to and do reflect to a considerable degree public policy and concerns about individual rights, so that I think the only power the Attorney General has in this area is, first the authorization and its restrictions, and second, his interpretation of what the Constitution allows.

Senator HUDDLESTON. What would prevent a future President or Attorney General from redefining a foreign agent or collaborator to include a political leader who might collaborate in a sense with a foreign government by lobbying his colleagues for support for that country, and meets with its officials?

Attorney General LEVI. I think the Constitution would prevent that. I am not sure that that is what your question is asking. I do not know how to answer a question which says there is a great deal of variety in political leaders and there is a great deal of history. Of course there is.

I suppose that is why we have the form of government that we do have.

Senator HUDDLESTON. It just occurred to me that a political enemy of a President or Attorney General that may have had some foreign contact could be brought under this as a potential collaborator, and therefore be subject to surveillance.

Attorney General LEVI. I included in the statement that one of the procedures that has to be worked toward is to make sure that there is no partisan political purpose. I am sure, speaking from what I know, there is none. I cannot obviously talk about these other areas.

The CHAIRMAN. Senator Schweiker.

Senator SCHWEIKER. Thank you, Mr. Chairman.

Mr. Attorney-General, one of the concerns of this committee as related to the warrant requirements is that the more deeply we got into the various intelligence agencies, CIA, NSA, and FBI, there seems to be a failure in the system to go before any kind of neutral magistrate to make a determination about such requirements. And the result is, of course, because that fail-safe system is not in operation, that we have illegal activities such as mail opening, listening, and black bag jobs. I'd like to ask you, as Attorney General, what is currently being done in the Justice Department to give you some kind of a better check, better control, better feel of the situation in terms of ferreting out possible illegal procedures and making certain that they are followed up as to what happens in the future?

Attorney General LEVI. As far as the Federal Bureau of Investigation is concerned, there are memoranda from me and from the Director which have asked that all activities which might raise any question of impropriety be called to my attention. Insofar as you are talking about what goes on in other agencies, what I think you are referring to are violations of law. We have criminal prosecutions and we have investigations in process now.

Senator SCHWEIKER. The problem here in the case of both mail opening and NSA interceptions—I believe the testimony shows that the Attorney General did not know about the mail openings until 1973 and the NSA interceptions until 1975. So we have seen a breakdown in the system in terms of your people being aware that these things were going on for 20 or 30 years.

Attorney General LEVI. Well—

Senator SCHWEIKER. I'll say your people. I am talking about the system.

Attorney General LEVI. It seems to me that the kind of items that you are describing usually require presidential authorization of some kind or another and I would hope in the future that any such presidential authorization or intended authorization would be passed upon by the Attorney General.

Senator SCHWEIKER. The problem was that it did not have presidential authorization. In the case of mail opening I do not believe we had any testimony specifically linking it to a President. This was one of the troubles. The system seemed to break down because it does not go up the chain of command at present. Apparently, in most cases not to the Attorney General either. It seems to me it places a larger burden on the Attorney General and the Justice Department to have a way of checking this, finding it out, ferreting it out. That is the point I'm trying to raise.

Attorney General LEVI. As I say, I do not understand unless there is Presidential authorization on the mail openings, for example, or the kind of case where you can get a warrant. I am not sure how that differs from any other kind of violation if in fact they occur. There is always the problem about authorization. I would not be so sure about who, after a great many years have passed, has the burden. I really should not discuss that, the question of authorization. If you are saying do I know some automatic way, no; I do not.

Senator SCHWEIKER. Let me put the question another way then. How would you feel about an Inspector General's office under your direction that would have this responsibility?

Attorney General LEVI. That would roam around the Government?

Senator SCHWEIKER. To the areas that you would normally have jurisdiction for prosecution if there were illegal procedures. It seems to me that something is missing in our government procedures. That information has not gotten to the Justice Department so that action could be taken. The CIA has an Inspector General. The question is whether the Attorney General should have for his procedures an Inspector General procedure of some kind.

Attorney General LEVI. The argument that is being made is that the Inspector General worked so well with the CIA, that the Department of Justice should also have a similar, perhaps a more general Inspector General? I really think what is involved is, first, the morality, which is perhaps not the right word, of the administration of the country. I say it is not the right word because I am very conscious that many of these things were begun at different times with different spirit and feeling of importance and what not. But, second, the enforcement of the criminal law. And I think that has to be pursued vigorously. I am not sure that an Inspector General would make any difference in terms of the investigation because the investigation would be conducted for us, as you described it now for the other agencies, by the FBI.

Senator SCHWEIKER. Let me focus maybe even more specifically on my question. Part I, section 9 of the FBI manual, for example, which is entitled "Disciplinary Matters," has this section in it. I would like to read it. This is a matter of the policing of possible areas of possible illegality. It's entitled "Disciplinary Matters."

It reads, and I quote:

Any investigation necessary to develop complete essential facts regarding any allegation against Bureau employees must be instituted promptly, and every logical lead which will establish the true facts should be completely run out unless such action would embarrass the Bureau or might prejudice pending investigations or prosecutions in which event the Bureau will weight the facts, along with the recommendation of the division head.

I think the attitudinal problem, the intrinsic institutional problem, here is a built-in procedure, that if it's embarrassing to the Bureau, that investigation is aborted. I'm talking here to the FBI. Frankly, I can make just as strong a case for CIA as someone else. I do not want to single out the FBI.

It seems to me as long as you have that attitude within the Government by enforcers and people who look at others for laws, we really have some problems. If it is embarrassing, do not pursue it, do not follow it up, do not investigate, abort. What is your response to that

attitude, that situation? Do you agree with that statement? Should that be a part of the FBI manual?

Attorney General LEVI. Senator, I assume you know I do not agree with the statement. First, I do not know when this delightful statement was written. Statements of this kind have been in the Government long enough, I know get written, and there they are. They do remind me when I was in the Antitrust Division, of similar statements written by employees of companies, and obviously, it is a foolish and wrong statement. I am sure that it does not reflect the present policy or attitude of the Bureau.

On the whole, I think it is a rather good thing that you have this document and that I have it and that one can use it to make the point which I suppose has to be repeatedly made. But I can assure you that as far as I know, that does not represent the present position of the Bureau in any way. I have not seen this before. That should not surprise you. There are a number of these things I have not seen. I am glad to see it. I suppose that this is one of those actions that would embarrass the Bureau and so they will have to deal with it. It is a little unfortunate, I think, because I am sure the present leadership of the Bureau is not reflected in the slightest in this statement. Of course I am opposed to this statement.

Senator SCHWEIKER. To be fair, Mr. Attorney General, we did alert you this morning that I was going to make this point so you would have a response.

Attorney General LEVI. To be fair, that is really not the case. To be fair, I was alerted when I sat down here after lunch and I had no opportunity to check it whatsoever. I did not make any point of it, because it would not have made any difference.

Senator SCHWEIKER. We did call the Bureau this morning, Mr. Attorney General. They came back with a statement to me. I assume they came back to you around lunch time. My only point is we first talked about this esoterically, theoretically. You say you do not really see a need for an Inspector General's office. You do not see a need to police it. I'm getting very specific. I think intrinsically and institutionally that there is a heck of a problem and we have it here and this is just part of it. I am not pinning it on the FBI or CIA.

Attorney General LEVI. The Bureau does have a very active inspection system. The Department of Justice when there is an allegation of wrongdoing—we establish a separate group to look into it. So really it becomes a question—I am not arguing about the means.

Senator SCHWEIKER. I asked you that just 5 minutes ago.

Attorney General LEVI. Then I do not understand the question. I thought the question was, should we have an Inspector General in the Department of Justice for the entire Government. I thought that was what your question was.

Senator SCHWEIKER. Both.

Attorney General LEVI. As to the letter, it seems to me that the Department of Justice's function, when it is not referred to as a matter of law, would be a violation of the criminal law, and we have to be vigilant in the enforcement of criminal law.

Senator SCHWEIKER. What we are dealing with is an intrinsic, inherent institutional problem. In one of the other hearings we had on black bag jobs, a memo again said that in essence black bag jobs are

justified. The special agent in charge must completely justify the need for the use of the technique—black bag job—and at the same time assure that it can be used safely without any danger or embarrassment to the Bureau.

The point that I am making is that the criteria seem to be not what the facts are, not what the legalities are, not what the integrity of the system is, not what the enforcers ought to be doing, but is it embarrassing?

As you look through here, this is really the whole thrust, and to push it off and say: "Gee whiz, we do not need an Inspector General, we do not need this, we do not need that," is to ignore the whole mountain of evidence the other way. I think it is the job of this committee to point this out. I think it is the job of all of us to see if we cannot find a better way of giving assistance.

I do not want to say the FBI—I want to make it very clear you can make just as strong a case against any intelligence agency you would look at. It just so happens that we have something in terms of specifics. To say that there is no problem, to say that we do not need a system, to say that we do not seek some kind of inspector, is to say we do not have to take a look at it. I honestly do not think it's realistic. That is all I have, Mr. Chairman.

Attorney General LEVI. I wish to say that the Attorney General did not say those things.

Senator SCHWEIKER. I would like to insert into the record a statement provided to me by the FBI which is the Bureau's explanation of the provision in the present manual that I have been referring to.

[The material referred to follows:]

The FBI's Manual of Rules and Regulations; Part I, Section 9: Disciplinary Matters; Item C: Investigation; states as follows:

"Any investigation necessary to develop complete essential facts regarding any allegation against Bureau employees must be instituted promptly, and every logical lead which will establish the true facts should be completely run out unless such action would embarrass the Bureau or might prejudice pending investigations or prosecutions in which event the Bureau will weigh the facts, along with the recommendation of the division head."

The statement, "unless such action would embarrass the Bureau," means that in such eventuality, FBI Headquarters desires to be advised of the matter before investigation is instituted so that Headquarters would be on notice and could direct the inquiry if necessary.

The statement, "unless such action . . . might prejudice pending investigations or prosecutions in which event the Bureau will weigh the facts" means that in such cases, FBI Headquarters would desire to carefully evaluate the propriety of initiating or deferring investigation of a disciplinary matter where such investigation might prejudice pending investigations or prosecutions.

Nothing in this Manual provision is intended to deviate from the FBI's established policy of conducting logical and necessary investigation to resolve possible misconduct on the part of its employees.<sup>1</sup>

Senator HART of Colorado. Mr. Attorney General, just an observation of your statement: Much of the case law you presented, and the policy discussions over the years relate to unauthorized use of information by Government employees, FBI agents, or whatever, carrying out surveillance, wiretapping, and so on. One of the reasons that this committee sits and you are here today is the changed circumstances, the situation where the highest officials of our Government use the instrumentalities and the information they gain for whatever purpose,

---

<sup>1</sup> See Appendix, page 164.

largely for political purposes, often for an illegitimate purpose. What we want to do is address that problem, which is at least in my mind utmost, rather than the problem of the random FBI agent, Justice lawyer, U.S. attorney, or assistant U.S. attorney somewhere, who may strike out with a little bit of information he picked up. We are concerned about the frontiers here and consequently I think your thoughts on the question of warranted versus warrantless search and seizure, are extremely important to us.

I noticed at the beginning of your statement in this connection, you talk about your present policies of authorizing electronic surveillance, and interestingly enough, of the four categories you mentioned, two start off with the purpose of protecting, and two start off with the purpose of obtaining. I personally have very little problem with the two, starting off with protect. I have more problem with the two that talk about obtaining—"to obtain foreign intelligence deemed essential to the security of the Nation." That, as I am sure you would admit, is a very, very wide category. Although your statement is limited to electronic surveillance, it could be broadened to the breaking into embassies and a lot of other things. Do you feel competent to determine, even with the structure established under you, what is essential to the security of this Nation?

Attorney General LEVI. I feel competent to pass in a legal way on whether the kind of certification which has been given to me and to my staff, along with such responses to questions of importance which we may have, so that we are sure that the certification is taken seriously and so that we can have some measure of the importance. Yes; I feel competent to do that. I am sure that a different answer would be that the intelligence people would think that I was quite incompetent to do it.

Senator HART of Colorado. Would you feel equally comfortable with this procedure if you knew your successor were a highly politicized Attorney General, appointed by a President in which you had little confidence, whom you suspected would use this procedure to further his own political purposes?

Attorney General LEVI. I would never feel comfortable with people in high office if that is what it is, distorting the law for political reasons.

Senator HART of Colorado. There is no law here. This is the problem we are talking about.

Attorney General LEVI. That is not my view in the slightest. I think that there is law. I do not know how one defines that. There are cases; they make law.

Senator HART of Colorado. What cases would you refer to, to instruct you as to what is essential to the security of the Nation? We are talking about judgment here, factual judgment.

Attorney General LEVI. All right. That happens to come, that language comes from the proviso which Congress wrote into title III. And I suppose it would be the same law if Congress, in writing it in, had provided some kind of a procedure to implement it. We would still have to make that determination.

I do not know going back to—you asked me really two questions. One is am I competent to make that determination or members of my

staff; and second, how would I feel about someone who is distorting judgments for political reasons or something. I think speaking in this political forum, I always feel uncomfortable if legal matters, if the interpretation of this phrase in a sense is a legal matter, are distorted. But I think that the constructive problem is, if this is not the best way to do it, to find the best way to do it. I tried to discuss in the paper how one would do it if you went to a judge for a warrant; on that you would have exactly the same kind of a problem. It might be worse.

Senator HART of Colorado. How about a congressional oversight committee to which you brought these requests and consulted with them to share that burden?

Attorney General LEVI. That strikes me as raising both of the questions that you asked me. First, the one of competence and second, a political view. So I do not know what to say. You have had more experience than I have had on such matters, about whether that would make it more or less political. And the second question, I do not know if the information is secure. I cannot answer that either. Whether that would be some kind of a check, I do not know—that kind of a procedure as mentioned in the paper is followed in some foreign countries.

While I have not given—and I rather doubt whether a congressional oversight committee might want the specific job of passing on a warrant or an authorization, which I would not regard as oversight at all. I do not know what you would call it. I do not know whether you would want that. I have reported to what I regarded as the appropriate, so-called oversight committees, mainly the Judiciary Committees, quite precisely, on wiretaps and microphones. The question is how far one goes with that. I do not know whether it is the congressional oversight function to pass on a particular warrant. That may be. That seems to me to raise serious constitutional problems.

Senator HART of Colorado. I take it your answers so far would apply to the fourth category, also to obtain information certified as necessary for the conduct of foreign affairs. Does that include, let us say, a Secretary of State who is concerned about members of his staff talking to the press?

Attorney General LEVI. Certainly not.

Senator HART of Colorado. Certainly not?

Attorney General LEVI. Certainly not.

Senator HART of Colorado. Well, if to the degree that conduct of foreign affairs is being jeopardized or was thought to be jeopardized by possible leaks from within the staff, I would think obtaining information about that would be important, would it not?

Attorney General LEVI. If you think that, Senator Hart, I really have to worry about the procedure that you are suggesting about having it go to an oversight committee.

Senator HART of Colorado. I did not suggest it. I was merely asking your opinion.

Attorney General LEVI. My opinion would be it would not.

Senator HART of Colorado. Why is that?

Attorney General LEVI. I do not think that that is an appropriate way to read that kind of doctrine against the background of what I tried in this paper to describe as the reach of the fourth amendment. I would think it quite inappropriate and a violation really of what

the *Keith* case is talking about. I cannot believe that either you or I—

Senator HART of Colorado. I am sorry. We have some dangling answers here. I am not sure I understood what you said.

Attorney General LEVI. Apparently I misunderstood you. I thought you said that a scrutiny of a newspaperman as to whether he was getting leaks, whether that was necessary for the foreign affairs matters and national security of the United States, would that be uncovered? I misunderstood you to say that you thought it would be. That shocked me.

Senator HART of Colorado. I was asking a rhetorical question. Again, we have the problem that we don't know what your successor would think.

Attorney General LEVI. We do not know who he is, I presume.

Senator HART of Colorado. If the Secretary of State were to come to the Attorney General and say, "a member of my staff is talking to the press about matters important to the conduct of foreign affairs"—you say you would not grant it. We do not know whether your successor would.

Attorney General LEVI. It is unconstitutional.

Senator HART of Colorado. I hope your successor feels the same way.

Unfortunately, I have to go vote. We will bid you good day. Thank you very much for your participation.

[A brief recess was taken.]

Senator MATHIAS. Mr. Attorney General, you have chosen to visit us on a very peripatetic day. We seem to have difficulty in arranging our meeting so we do not stumble all over each other.

I was interested in several of the facets of the statement. One, in which you refer to the Constitution as emanating from and applying to the people. And I do not think any of us seriously challenges that as a concept. But I guess the difficulty arises, when do you decide that a certain American is no longer one of the people?

And let me ask the question, maybe more specifically, if an American citizen is charged with foreign espionage, does that separate him from the people?

Attorney General LEVI. No. Of course the fourth amendment applies to it, as do other constitutional protections. I think that was not really intended to be the thrust of that paragraph.

Senator MATHIAS. So that the mere charge or serious suspicion on the part of the law enforcement authorities would not suspend the protections of the fourth amendment?

Attorney General LEVI. Senator, if I may so say to sharpen it, the question is whether you think it applies to foreign nations. And all I was suggesting was that its application must at least take account of that difference.

Senator MATHIAS. Also in your statement, you refer to the fact that at the same time, in dealing with this area, it may be mistaken to focus on the warrant requirement alone to the exclusion of other, possibly more realistic, protections. That could get us into days of discussion on what more realistic protections are. I was more interested that there seemed to be a cross-reference between that and another line in which you refer to the Canadian experience, in which one of the other more realistic protections was the report to the Parliament of the number

of national security surveillances initiated, their average length, a general description of the methods of interception or seizure used, and an assessment of their utility.

You and I, on a previous occasion, discussed a bill which I had introduced which in fact calls for this very kind of a report to the Congress. I wonder if you would like to enlarge on either of these references?

Attorney General LEVI. I think that is a possibility, and I said, I think when you were not here, that I had, in fact, made something of a report that was made public to the Judiciary Committee which gave some of this information. Now, my guess is that the Solicitor General files in Canada are in fact, quite general, and it is probably somewhat the same as my letter, although mine did not include an assessment of the utility. When you were not here, Senator Hart was asking me how I felt about having a so-called oversight committee, if I understood him correctly, to determine whether a warrant or authorization could be given. That seemed to me to mix up all parts of the Government even more than they are now, and to raise security questions and so on. It is obviously something one can think about.

Senator MATHIAS. In somewhat the same area, Kevin T. Maroney who is your Deputy Assistant in the Criminal Division testified in the House and argued against a requirement of judicial warrant in all national security cases. One of the grounds he advanced was the question of the competency of judges, who are perhaps not that accustomed to dealing with foreign policy matters, to evaluate the affidavit of a person who is a foreign intelligence expert. It is a long time since I earned a living at the law. My recollection is, we impose on judges a task of evaluating a wide variety of technical questions on matters that deal with industrial processes, with surgical procedures, with traffic patterns, with environmental questions. Would you not think that a judge could evaluate an affidavit that the person who was a foreign intelligence expert as he does other expert testimony?

Attorney General LEVI. I think that there would be some problems. In the first place, it would be hard to get a doctrine of common law on the subject, because opinions could not really be written. A great deal of the material would be extremely confidential.

Since I concluded that portion of my paper, not Kevin Maroney's, by saying that I thought that a judicial warrant would give a greater sense of security to the country, I do not want to overpress the point that it would be difficult for judges to make the kind of determinations that would be necessary. I would say that I would assume that they would have to spend as much time on it as I do, and would have to have as much a staff on it as I do, which is considerable, and that there would be security problems, and so on and so forth, and the security of the judge. So that, I also think that the judges undoubtedly would respond to this in general by having broad categories where they automatically, where I do not, give the warrant. I think that that is a fact. I do not say that because I wish to keep for myself or my successors this undelightful duty. I think it is something that you have to take account of, though, in thinking about the legislation.

Senator MATHIAS. You have been very patient with us, I must say, in spite of the fact that your voice is still very strong and vigorous—

Attorney General LEVI. It is because of electronic surveillance.

Senator MATHIAS. Without pressing you on that point, I would say that it does concern me that an American has less protection because the "probable cause" standard does not exist if there is a suspicion of a national security interest in the case.

Attorney General LEVI. I think the fact is that at the moment Americans have much more protection under the procedures that we have devised than they do under title III.

Senator MATHIAS. That is a subject that will be debated, I think.

The CHAIRMAN. You are talking about your Department, are you not, and not the NSA?

Attorney General LEVI. Yes; that is all I am talking about.

The CHAIRMAN. You are just talking about the Justice Department?

Attorney General LEVI. That is correct.

Senator MATHIAS. I have two very brief other questions. I am just wondering if, in your view, the constitutional powers in the area of foreign intelligence are exclusive to the Executive or whether they are concurrent with the legislative branch?

Attorney General LEVI. They are sufficiently concurrent so that legislation by the Congress would be influential. You have an example of it, because the wording of the President's memorandum, while not identical, so closely follows the proviso that Congress wrote. You are asking me whether I think there is presidential power beyond that, and my answer is, "Yes."

Senator MATHIAS. Finally, and I realize this might be asking you to make a statement against your interests, whatever way you answer: Do you think the Attorney General ought to be a statutory member of the National Security Council?

Attorney General LEVI. I have never thought of that. Up until the present time, I have been delighted that I have not been.

Senator MATHIAS. If you think further of it and care to share your thoughts with us, we would be glad to hear them.

The CHAIRMAN. One final question from me. I have listened to the discussion of how one set of procedures, a traditional set of procedures involving courts and warrants, has developed in the criminal field; how a very different set of procedures exist in the intelligence or national security field; how, in the latter field, people could be watched and listened to without knowing in any way that their rights had been trespassed upon by a less scrupulous Attorney General than yourself, or a less scrupulous administration; and how there is nothing outside of the executive branch to check on it, and in this way it is different from the ordinary practices in the law; I think it is potentially very dangerous. You can fall back on the argument that good men will establish and follow good procedures, but there is no one outside the executive branch that can check on any of this, and I should think that there ought to be. Maybe it is not a judge that has to give a warrant. That may not be the practical way of dealing with it. Maybe it should be an oversight committee of the Congress that exercises jurisdiction over such matters, a committee that can ascertain to its own satisfaction that procedures are being followed and the laws, whatever they may be, are being adhered to.

The question I have relates however to the FBI. I sometimes think that the FBI has a kind of Jekyll and Hyde complex, in the sense that when it is dealing with law enforcement matters it has these rather

traditional procedures that it must adhere to; but when the same agency deals with the counterintelligence, national security, it is living in a different world. Would it be sensible to break the Bureau in two so that the part that deals with traditional law enforcement is that, and that alone, and that another department within the Justice Department and under the Attorney General would deal exclusively with national security and counterintelligence matters, that are really quite a different character than normal law enforcement?

Attorney General Levi. Obviously, that is not a question that one answers without a great deal of thought. My own present view is that it would not be a good idea, because the point is to develop procedures which are adhered to just as vigorously in both areas. This is one reason we do have a committee which has been hard at work fashioning guidelines. These guidelines, when completed—I think the committee has seen some of them—will be in statutory or Executive order form.

But I think, whatever the shortcomings may have been in the past, that a strong attribute of the Bureau is its discipline, and that one wants to develop in this area—where, by the way, it is wrong in some sense to fault agencies when the law changed as it did. It would be desirable to develop procedures in that area which would evoke the same discipline and, although the area is quite different, there are comparable points, the checking, the reviewing, the getting permission, and so on. It is really a different world. One of the problems, Mr. Chairman, if I may say so, is when one looks at the past, one finds some terribly interesting things, but sometimes one forgets what the present is like.

The CHAIRMAN. I will not belabor the point, except to say when one agency does both kinds of work, I think that there is some danger, although it may be well-disciplined, for the methods in the one area to creep into the other. It may be more sensible to let counterintelligence and national security matters of that kind be handled by a separate bureau under the Justice Department. I would not want to see it all thrown into the CIA, for example; I want them to look outward in dealing with foreign countries, and not dealing with this country. But a separate department within Justice that deals with this quite separate matter from ordinary law enforcement, is an idea which I think should be given more thought.

Thank you very much for your testimony.

Our next witness is Prof. Philip Heymann of the Harvard Law School.

[The prepared statement of Prof. Philip Heymann in full follows:]

**PREPARED STATEMENT OF PHILIP B. HEYMANN, PROFESSOR OF LAW, HARVARD LAW SCHOOL**

**I. INTRODUCTION**

A. This Committee has heard evidence about a number of activities of the intelligence agencies which raise significant questions.

1. Two forms of activities are familiar:

a. Surreptitious entries.

b. Domestic electronic surveillance.

2. Two other forms of activity were previously unknown and raise comparatively novel questions:

a. The opening of mail to and from the United States.

b. The interception of cable and phone communications between the United States and foreign countries.

B. These activities and others the Committee has reviewed raise three sets of questions. I shall address only the last of the three, not because the others are unimportant or even less important but because time does not allow dealing with all of them on a single occasion.

1. There is a serious question about the collection of files on dissenters. I think there can be no serious doubt that an operation such as the "CHAOS" operation of the CIA tends to discourage participation in legitimate political activities, particularly by those who are somewhat timid. The Army intelligence gathering program raised similar questions.

2. Wholly separate from the question of the chilling effect of an excessive collection and maintenance of files, there are the unique problems that are created when intelligence agencies such as the CIA and NSA wander into the domestic area. These agencies are unlike our domestic investigative agencies in a number of relevant ways.

a. They are funded in the billions of dollars.

b. Their employees are trained to operate in secret circumstances abroad and without necessary conformity with local law.

c. The importance of secrecy makes the monitoring function performed for domestic agencies by the Congress, the courts, and the public at large much less applicable.

These characteristics led the Congress to attach a statutory prohibition to domestic activities of the CIA. I am aware that members of the Committee pressed General Allen on whether this would not also be desirable for the NSA.

3. The third subject for the Committee's concern, and the only one I intend to address today, is the problem of invading the privacy of communications of American citizens. This is an area that the Fourth Amendment of the Constitution and a number of statutes protect. In discussing this area I will attempt to make clear where the law is moderately firm and where it is uncertain. I shall also do my best to separate off my recommendations from my estimates of what the law is.

C. As we proceed to discuss these questions, it will become apparent that additional legislation would be highly desirable for several reasons.

1. We are dealing with the area of foreign policy and most particularly with the special situation of intelligence gathering and secret technology. This Committee and through it, the Congress, have a factual basis for assessing these matters which courts cannot duplicate. This is especially true after the Committee's extended set of hearings.

2. There are obvious and important gaps in the present law which legislation will be needed to fill. I will allude to these as I proceed.

## II. THE EFFECT OF A GOVERNMENTAL INTEREST IN FOREIGN INTELLIGENCE ON THE FOURTH AMENDMENT RIGHTS OF CITIZENS

A. One question runs through each of the areas the Committee has been investigating: to what extent does the Fourth Amendment apply to matters of national security?

1. There are a series of additional difficulties to be addressed in connection with searches of international mail and international voice and non-voice communications.

2. But the same question as to what difference is made by a foreign intelligence objective applies to those programs as well as to more familiar searches of homes, offices, or domestic communications.

B. The Fourth Amendment provides two different forms of protection, each of which could be affected by the fact that the government is pursuing a foreign intelligence interest.

1. Through its requirement of a judicial warrant absent certain long-established exceptions for emergencies and arrests, the Amendment imposes a more neutral evaluation of the situation between a governmental desire for information and the action of engaging in a search. It also, equally significantly, requires a written, sworn record of the basis on which the search is undertaken.

a. It is important to emphasize, as Justice Powell did in *United States v. District Court*, that the fears the framers had in mind included not only invasions of privacy but also the use of a search to silence dissent.

b. The classic language here is that a detached, neutral judicial officer should stand between an over-eager executive branch and the rights of citizens.

2. The Fourth Amendment also imposes certain requirements of probable cause and sensible procedures.

a. In this area there has been a great deal of fluidity. Less probable cause is necessary if the intrusion is less or if the threatened harm is greater.

b. Such requirements as notice of the search have been held to be subject to reasonable modifications as in the case of the Wiretap Act where no notice need be given for ninety days and even then it can be delayed if this is essential to an investigation.

C. The simpler part of the question as to the impact of national security concerns on the Fourth Amendment goes to the need for a warrant at all. This part may be the more important nonetheless, for on our trust in the neutrality of judges turns a great deal of the citizens' sense of security as well as a real protection against unjustified attacks on dissent or a simple arbitrariness.

1. With the concurrence of judges from the most conservative to the most liberal wings of their benches, the courts have by now gone far toward answering the question as to the necessity for a warrant in national security areas.

a. First the Supreme Court held in a unanimous opinion by Justice Powell that the President had no power to dispense with the warrant in the area of internal security. Justice Powell emphasized the dangers to dissent.

b. Then after two courts had sustained surveillance without a warrant of diplomatic establishments and non-citizen foreign agents, the D.C. Circuit in *Zweibon v. Mitchell* has held unanimously that, at least wherever the party being monitored is neither a foreign agent nor a collaborator with a foreign government, a warrant is required for a wiretap even in the pursuit of foreign intelligence or foreign policy.

c. Note that this leaves the government free to search without a warrant in the cases of embassies and non-resident employees of foreign governments.

d. This area is one to be regulated by diplomacy, not by the Fourth Amendment.

2. The courts' reasoning has been, I believe, persuasive.

a. The rules as to probable cause and necessary procedures can be adjusted in such a way that the requirement of a warrant protects against malice, arbitrariness, or attacks on dissent without limiting the government in its pursuit of legitimate goals.

b. The history of the Fourth Amendment involves a number of searches in the national security area where, in important cases, warrants have been required.

c. The notion that courts are unable to understand enough of the situation to exercise a meaningful review function is implausible, especially when one recognizes that the Attorney General exercised that function for the executive branch. Moreover, there is no real risk of revealing secrets. The record of courts in this regard is far better than that of the executive branch.

d. It is my understanding that the Attorney General has now accepted the position of the D.C. Circuit at least for the time being.

3. These cases leave open three questions that the Committee could well address:

a. No court has yet held that an American citizen or resident alien—as opposed to an embassy or foreign employee of another nation—who is found to be a foreign agent or collaborator can be searched without judicially determined probable cause to believe he has committed espionage, sabotage, or some other crime. Both the Supreme Court and the D.C. Circuit have left that question open. Should there be such a category? The case against it is that the Congress has prohibited and can prohibit any conduct it considers dangerous to our national security and that no action should be taken against a citizen until there is reason to believe he has violated (or conspired to violate) such a prohibition. The case for an exception is that secret foreign agents are an important source of positive information about intentions of other governments and about other agents even when they are not yet engaged in illegal conduct.

b. If there is to be such a less-protected category of citizens who are secret agents, what should the definition of foreign agent or collaborator be when we are dealing with American citizens? It cannot, for example, open to electronic surveillance the telephones of any law firm which represents the government of France or Bolivia. A statutory definition would have to involve the secret acceptance of pay or directions from a foreign government.

c. Perhaps most important, if there is a category of American citizens who are foreign agents or collaborators and which receives less protection under the Fourth Amendment, should there not be a requirement that the status of foreign

agent or collaborator, as defined by Congress, be determined by the courts on a warrant. The excessive suspicions of Presidents Johnson and Nixon that anti-war dissent was controlled from abroad led to the CHAOS program. A sensible protection against any recurrence would be to require a judicial warrant based on a sworn affidavit establishing that a citizen is a foreign agent. This is obviously a highly important protection when organized, legitimate disagreement with government policy is involved.

D. The second aspect of the question whether a foreign intelligence interest makes a difference to Fourth Amendment protection is harder. It raises the question whether in the case of citizens who are not foreign agents or collaborators with a foreign government there is any right to search simply to obtain foreign intelligence and not only, as traditionally, with probable cause to believe that evidence of a crime will be found. On analysis, it seems clear to me that no such right should exist, although the case law is not helpful one way or the other.

1. Put in its clearest form, the question is this. Assume that an American industrialist or banker has returned from an unfriendly country with knowledge that would be very valuable to our intelligence agencies regarding the industry or finances of the foreign country.

a. Certainly it is proper to ask the American citizen to reveal that information and indeed we presently do.

b. But what if that extremely important foreign intelligence is withheld by the citizen for any of a number of reasons. Can he then be made a subject of electronic surveillance or can his home and office be searched if the information is important enough? The question, quite starkly, is whether there should be a warrant procedure that allows searching entirely loyal Americans whenever there is probable cause to believe that they possess important foreign intelligence which they will not reveal freely.

2. I believe the answer to this question is that the matter should be handled by legislation, if at all, and not by executive discretion. Although the merits of the proposal are highly questionable, the Congress might:

a. Make it a crime to fail to turn over certain well-specified classes of information. If it did, there would then be probable cause to search for and seize such information if it was not turned over.

b. In the alternative, the Congress could make a well-defined class of information subject to subpoena.

I don't recommend either of these alternatives, but they are obviously preferable to an undefined executive discretion to search entirely loyal American citizens. If the matter is to be handled at all, it should be by legislation.

3. There is indeed case law that indicates that a search of an innocent party is improper unless there is reason to believe that the evidence will not be turned over voluntarily or in response to a subpoena. This case law would also suggest that only a well-defined class of foreign agents (who could not be expected to comply with a subpoena) might possibly be subject to electronic surveillance in order to obtain valuable, positive intelligence in situations where there is no reason to believe that they have committed or are about to commit a crime.

### III. THE ADDITIONAL DIFFICULTIES PRESENTED BY THE PROGRAMS OF MAIL OPENINGS AND INTERCEPTION OF INTERNATIONAL COMMUNICATIONS TO AND FROM THE UNITED STATES AND INVOLVING UNITED STATES CITIZENS

A. Wholly aside from the special questions with regard to a possible foreign intelligence exception to the Fourth Amendment rights of American citizens, there are a series of difficult problems presented by the testimony the Committee has received with regard to mail openings and interception of international communications. I will address three of these in an order of increasing difficulty.

B. Fourth Amendment rights only pertain to American citizens in a situation where they enjoy a reasonable expectation of privacy with regard to their communications.

1. The situation with regard to mail is unusually clear.

a. The germinal case dealing with Fourth Amendment protection of the mail was *Ex Parte Jackson*, 96 U.S. 727 (1878) in which the court held that while in the first class mail, papers can only be opened and examined under a search warrant. This rule which was reaffirmed as recently as 1970 in *U.S. v. Van Leeuwen*, 397 U.S. 249, is now embodied in a federal statute, 39 U.S.C. 4057. It provides that "only an employee opening dead mail by authority of the Post

Master General, or a person holding a search warrant authorized by law may open any letter or parcel of the first class which is in the custody of the Department."

b. The only possible questions involve whether a U.S. citizen is protected as a recipient of mail from a foreign resident, or is only protected as the sender of mail. For four reasons I believe it is moderately well established that the recipient is also protected.

(1) A number of cases have indicated that there is such protection subject only to a reasonable customs power. See, e.g., *U.S. v. Sohnen*, 298 F. Supp. 51 and *U.S. v. Various Articles of Obscene Merchandise*, 363 F. Supp. 165; *State v. Gallant*, 308 A.2d 274.

(2) 39 U.S.C. 4057 seems to clearly cover the recipient as well as the sender.

(3) The modern law with regard to the privacy of oral communications protects all the parties to the communication and would probably be read to apply to all the parties to a written communication as well.

(4) The recipient of a letter has something very close to a possessory claim to the paper on which it is written.

2. I believe the situation with regard to voice communications involving an American citizen and with one terminal in the United States is equally plainly covered both by the Constitution and by the Omnibus Crime Control and Safe Streets Act of 1968.

a. The definition of "wire communication" in the 1968 Act includes any communication made through the use of facilities for the transmission of communications by cable by any person engaged as a common carrier in providing such facilities for the transmission of foreign communications. The definition of common carrier plainly incorporates international communications to and from the United States.

b. Presumably the definition of "oral communications" would be read to be consistent with that and would therefore include radiotype voice communications.

3. The situation with regard to non-voice communications is less clear, but I believe there is every indication that they, too, would be considered protected under the Fourth Amendment.

a. As a matter of a reasonable privacy in expectation of communications, the only difference from voice communications is the extent to which a cable is revealed openly to a transmitting company. This might make revelation of its contents to the government within the reasonable expectation of senders were it not for 47 U.S.C. §605, the old Wiretap Act, which still forbids the revelation of content except "in response to a subpoena issued by a court of competent jurisdiction or on demand of other lawful authority." Any other form of interception of a non-voice communication would be a violation of a reasonable expectation of privacy. I take it that the voluntary act of a common carrier in complying with a request by a government agency to turn over cable traffic would not satisfy the exception for "demand of other lawful authority," a phrase that is apparently intended to refer to the subpoena powers granted by Congress to various agencies. See *Newfield v. Ryan*, 91 F.2d 700. Certainly an interception without the assistance of the common carrier would be treated as an invasion of the privacy of communications. Still, I should quickly acknowledge that there are practically no Fourth Amendment cases dealing with the interception of communications either domestically or in international traffic.

b. I do not believe that the 1968 statute covers non-voice communications. Its definition of "intercept" requires "the aural acquisition of the contents of any wire or oral communication." Acquiring the contents of a non-voice communication would not be "aural." The only possible statutory prohibition is in 47 U.S.C. § 605 which first prohibits the interception and divulgence of radio communications and then states that "no person not being entitled thereto shall receive or assist in receiving any . . . foreign communication by radio and use such communication (or any information therein contained) for his own benefit or for the benefit of another not entitled thereto."

4. With regard to each of these forms of communication, the situation may be entirely different when there are two foreign terminals.

a. A channel of communication that is overwhelmingly used and controlled by foreign interests does not invoke a reasonable expectation of privacy by American citizens.

b. The only qualification here would be if American agents or foreign governments acting at their behest specifically targeted the foreign communications of an American citizen. Here there might well be a Fourth Amendment claim.

C. In one situation the result of all this seems moderately clear. If an intelligence agency wants to open the letters or intercept the international communications of a named American citizen who is the target of an investigation, it will have to get a warrant and either show there is probable cause to believe the citizen is committing a crime or, if the Congress so determines, show that he is a secret foreign agent and that the communication is likely to contain important foreign intelligence.

1. This alone disposes of many of the situations before the Committee.
2. The lack of a clear law dealing with non-voice communications suggests that the Committee would serve a real function by addressing this question directly.

D. The hardest question arises with communications that can, without a serious invasion of privacy, be checked for words or other selection criteria or, in the case of letters, for indicators on the envelope that tend to show that the communication may contain evidence of a past or prospective crime.

1. In the case of mail, looking at the outside of the envelope for indicators that it may contain evidence is not itself a search.

2. The difficult question arises if it turns out that the indicators will lead the investigative agency to read a number of innocent letters for each letter that contains evidence of a past or prospective crime. At this point, there is apparently no choice other than to either open the letter and invade the privacy of the sender and receiver or to leave it unopened although there is a probability that it contains evidence bearing on a substantial danger.

a. In traditional terms, the question is one of a general search. The Constitution was written to forbid general search warrants such as the Writs of Assistance were in colonial times.

b. There is no simple answer to when a search is too general. Any search involves a certain probability that it will not reveal evidence and every search, even where the result is that evidence is found, involves breaching the privacy of non-evidentiary matters. The question is always one of establishing a balance between the invasion of privacy and the need for the search. As always under the Fourth Amendment, if what is involved is a serious prospective crime, there is more room for a fairly general search.

3. The problem with international communications is similar, but may be subject to more of a technological solution. Consider the case of non-voice communications between an American citizen and an alien.

a. General Allen's testimony indicates that it may be possible to identify certain selection criteria without reading the entire message. These, like the indicators on the outside of a letter, would narrow the number of communications inspected and would increase the probability that any single communication contained evidence of a past or prospective crime. If this were done mechanically without reading all of the messages, there would not be a search during this stage of the operation.

b. When a narrower, but perhaps still excessive, class of non-voice communications has been identified, it may be possible to review these without revealing the name of the sender or receiver. Adding in that second step would substantially reduce the invasion of privacy.

c. It is also, of course, relevant whether the intelligence agency immediately discards any message that, on reading, proves to be innocent without keeping copies or records of the transactions.

4. The hardest question of all would be presented if: (1) an important part of the communications traffic on an international route to and from the United States does not involve American citizens; and (2) there is no way of sorting this part of the traffic from the part involving American citizens without a substantial invasion of the privacy rights of citizens. This might well be true with regard to voice communications, for example. Here there would be two questions to be addressed in sequence.

a. What procedures could be developed to minimize the intrusion on the privacy of American citizens, for example by quickly and completely discarding any communication involving American citizens and not revealing evidence of a crime?

b. What is the balance between the now-diminished invasion of the privacy of American citizens and the volume and importance of the purely foreign traffic involved? If, for example, ninety-five percent of the "take" were domestic and the remaining five percent pertained primarily to commercial matters, the balance would have to be struck in favor of forbidding the particular technique of intercepting international communications.

E. Obviously the questions I have just reviewed concerning the permissible techniques for monitoring international communications are matters which badly need legislative standards. In some cases, the nature of the program will be so clear and stable that Congress could itself define the requirements. In other cases, the Committee might well wish to consider a warrant requirement that first set forth general standards and procedures and then directed a court to approve a broad plan for monitoring a particular type of communications.

1. In either event, I would think it was highly desirable to require the intelligence agency to furnish on a continuing basis two forms of information.

a. Copies of any communications perused in their entirety with some indication of which ones were furnished to other government departments.

b. A numerical summary of the relationship between communications read but discarded and communications read and kept as part of any governmental program or file.

2. This will make it possible to estimate the extent to which the search is over-broad, the equivalent of a general warrant.

#### **TESTIMONY OF PHILIP B. HEYMANN, PROFESSOR OF LAW, HARVARD LAW SCHOOL**

Mr. HEYMANN. Mr. Chairman, I recognize it is late, and if I could submit my prepared statement for the record, I would be happy to try to summarize in a very few minutes what I have to say.

My objective, Mr. Chairman, is to try to state clearly the four or five or six issues that I think are presented by surreptitious entries, domestic bugging, NSA interceptions and mail openings.

I have had the feeling today that sometimes we are dealing with a large ball of wax called national security; sometimes we are dealing with 500 difficult little issues. My own view, and I hope I can convince you, is that there are about five or six different issues, and that this committee can address them individually with the result, I hope, that the law will be a little clearer when you are through. There are two types of issues. I want to break the categories into two, and then break them. There are certain issues that go directly to what the impact of foreign intelligence is on fourth amendment rights. Then there is another set of issues that involve what is special about international communications, mail, nonvoice cable, or voice.

Let me start with the question of what is special about national intelligence, foreign intelligence, because that one cuts through everything this committee has looked at. It cuts all the way from black bag jobs to sophisticated NSA items.

As you well know, there are two primary protections here, and foreign intelligence considerations could affect these. First, the fourth amendment has a warrant protection, to get a judge over an overly eager executive branch, if it is over-eager in a search. The warrant was there largely, as Justice Powell reminded us recently, because of fears as far back as the 18th century.

In the area of the warrant, the first part of what is special about intelligence, the courts have taken us a very long way toward a conclusion. First the Supreme Court, in the *United States v. U.S. District Court*, held that internal security required a warrant. Then the D.C. Circuit, in *Zweibon v. Mitchell*, in an opinion that the Attorney General has said he will live with, at least for the time being, has said even when the Government is pursuing foreign intelligence, it must get a warrant unless it's dealing with a foreign agent or collaborator. In other words, a great deal of the ambiguity the Congress left in

1968 is now cut down to the question, what happens with foreign agents and collaborators. As to that, I think that this committee has two very important questions to address, and it has been asking them of the Attorney General today. One question is: What should the definition of foreign agent or collaborator be? Senator Hart was pressing the Attorney General on that. It is not going to be an easy thing to draw up. If there is some special category of foreign agent and collaborator, it is going to take some work. It cannot include New York law firms who are representing Bolivia or France. It cannot include major Jewish organizations working in collaboration with Israel on a bond drive. It is going to take some work.

The second issue under the warrant that this committee is going to have to address is: If there is an exception for foreign agents and collaborators, should that be decided by the executive branch without a warrant, or should there be a warrant required where a judge decides that someone is a foreign agent, a citizen, a foreign agent or collaborator? Let me be clear that no one, including me or any court, is suggesting a warrant requirement for embassies or non-resident employees of foreign governments, all right? But what if the executive branch believes that someone is a foreign agent or a collaborator? Should not a court have to get into it? I would strongly urge that they should.

**THE CHAIRMAN.** Are you talking in this point, Professor Heymann, about bugging and wiretapping? The cases you have cited relate to those traditional methods.

**MR. HEYMANN.** I believe exactly the same standard would apply with regard to intercepting overseas communications, Senator Church. In other words, as I go about three steps down the line I am going to say to you that I think it is clear that international mail with a U.S. terminal, or U.S. citizen; international phone conversations, the same conditions; and international cable traffic, are all protected by the fourth amendment. I am going to give you cases and statutes that say that, and I am going to say that requires a warrant unless it is a foreign agent.

I hope that this committee says if the Government wants to say it is a foreign agent, it will require a warrant to certify that it is a foreign agent.

The second half of what is special about foreign intelligence is do you always need probable cause of crime, or can the Government sometimes go out, simply pursuing foreign intelligence. I think that you have to divide that one into two cases. One, with regard to foreign agents or collaborators, it makes some sense. There is a quite arguable position that for a foreign agent or a collaborator so certified by a court on a warrant, the Government ought to be able to pursue foreign intelligence, not just probable cause of a crime. The executive branch could live with a stricter standard, but there are cases that you can imagine and point out where a foreign agent would have information about a foreign country's plan that you wanted to pick up, with or without probable cause that the agent is committing a crime; or a foreign agent would make contact with other agents whose names it was important to know.

My sharpest difference with everything that the Attorney General was saying comes, I think, in the question, can the Government pick

up information from loyal, trustworthy American citizens by electronic surveillance at home, or through international means? Can it do that simply to get foreign intelligence when there is no evidence of a crime? Let me state the question very specifically: if David Rockefeller goes to the Soviet Union and learns information about their financial structure that the CIA would give a great deal to know, that it is very important to our foreign security, is there a right to bug David Rockefeller's phone to find out what he has learned? At the moment, as you know, we do make inquiries of David Rockefeller, and that is entirely proper. The question is if for any of a number of reasons he refuses to furnish that information, the foreign intelligence information that the executive branch wants, can his communications be monitored to find it out?

The CHAIRMAN. At home?

Mr. HEYMANN. I mean at home, by cable overseas, letter overseas, I mean by phone overseas, Mr. Chairman. It seems to me that the Congress has to face up to that rather directly.

The CHAIRMAN. Let us take the case of business transactions that may have an economic impact upon the United States. I would take it that if they were a transaction that involved foreign governments, investments, capital transfers and the like, that this would be within the right of the Government to obtain information through electronic surveillance methods, or any other method.

Mr. HEYMANN. The position that I am urging on you, Senator—

The CHAIRMAN. We are talking now about actions of foreign governments in the economic field.

Mr. HEYMANN. The question is whether the communications of an American citizen are monitored secretly to find out that information. I suggest to you that Congress would not pass a statute making it a crime to withhold valuable information, making it a crime for an American citizen to withhold valuable information, that Congress would probably not pass a statute authorizing an executive agency to subpoena that information. It would be regarded as the information of that citizen. If Congress were not to allow it to be done directly by criminal statute or subpoena, Congress should not allow it to be done indirectly by the executive branch monitoring an entirely innocent American citizen's communications.

The CHAIRMAN. Suppose that you are looking simply for intelligence having to do with messages of foreign governments.

Mr. HEYMANN Wholly?

The CHAIRMAN. You would have no problem with that?

Mr. HEYMANN. Foreign to foreign messages, I would have no trouble with, and foreign to foreign terminals, I have no trouble with.

The CHAIRMAN. How about messages between foreigners, as such, either abroad with both terminals abroad, or one terminal in this country and the other terminal abroad? Any trouble with that?

Mr. HEYMANN. Between two foreigners?

The CHAIRMAN. Yes.

Mr. HEYMANN. No, Mr. Chairman. There could be possibly a problem with resident aliens, but setting that minor problem aside—

The CHAIRMAN. Suppose in order to get the messages of foreign governments or foreign aliens with which you would have no problem,

it was necessary for technical reasons to take these messages out of the whole stream of messages.

Mr. HEYMANN. That is the hardest problem of all, Mr. Chairman.

The CHAIRMAN. Yes, it is.

Mr. HEYMANN. If I just may take three sentences to work up to the hardest problem. As I said to you, my statement makes clear that I think the law is absolutely solid that letters, including international letters, are protected. They have been protected by statute of Congress since 1825. The Supreme Court has held them highly protected for the last 80, 90 years. I think the law with regard to international voice communications involving American citizens is clear, constitutionally protected, and protected under the Safe Streets and Crime Act. I think the Wiretap Act applies to international communications if you look carefully at its definitions.

Mr. SCHWARZ. Do you mean with one terminal in the United States?

Mr. HEYMANN. With one terminal in the United States, that is the way the definition was.

Finally, I think the case is slightly less clear in regard to nonvoice communications. What this means, the second sentence that leads up to your hardest of examples, if these are protected communications, then you need a warrant. I think the Attorney General agrees with that, although he is hard pressed to say at this time, November 6, whatever date it is. If these are protected communications, the executive branch cannot read them or hear them without a warrant if what is being read, if what is being targeted is an American citizen. If somebody says I want to read Frank Church's international cables, there is a warrant requirement protecting it.

The hardest question, if what is being targeted is not an individual American, if it is an individual American—

The CHAIRMAN. To answer my question.

Mr. HEYMANN. That is the hardest question. As your committee has heard, the NSA has systems for identifying particular parts of the international traffic which are somewhat more likely to contain either evidence of a crime or foreign intelligence information than other parts. What if once it has identified a large, relatively large volume of traffic, that is suspicious? It will still be true that the investigating agency is going to have to read a great deal of that traffic in order to separate out perhaps perfectly proper foreign-to-foreign cables from American cables. Then what? My answer is really quite similar to the Attorney General's, if I heard him right, Mr. Chairman. The first question is what steps can be taken to minimize the invasion of privacy with regard to the protected cables involving an American citizen, an American terminal, or a protected phone conversation or protected mail? What steps can be taken to minimize the invasion? That includes, among other things, how quickly is the matter discarded, who sees it.

The second step which I think the Attorney General recognized this morning is you then compare the minimized—a court would have to and the Congress would have to—the minimized damage to American privacy with the importance and the value of the foreign-to-foreign traffic which is intercepted. If it turns out that 95 percent of the traffic is protected in the sense that it involves a loyal American citizen as one terminal in the United States, and 5 percent is foreign to

foreign, and the 5 percent is not of great value, say the 5 percent involves the price of grain; then the whole bundle would be unconstitutional.

**THE CHAIRMAN.** Who makes that judgment?

**Mr. HEYMANN.** The last question. It can only be done in one or two ways, I believe. If we are talking about a type of interception of communications which was very constant over time, Congress could go far to either declaring it legal or illegal. If we are talking about a type of interception that may change and be different next year than it is this year, Congress is going to have to lay down standards for courts to apply.

Now the Attorney General's statement this morning contains references to a number of cases where the Supreme Court has ordered and authorized courts to set up general principles and general procedures for handling fourth amendment questions. The most recent is Justice Powell involving Customs searches on the border of Mexico. The Supreme Court with Justice Powell speaking said, the lower court ought to say just when and where there can be inspections within 20 miles of the border of Mexico.

I believe that ultimately the Congress is going to have to pass a statute that sets forth standards and then requires a warrant from a court. Perhaps a warrant approving a monitoring system with a whole volume of traffic. It does not have to be a warrant for each individual bit. Congress is going to have to set forth the standards and courts are going to have to come in and apply them.

Finally, I think it is very important that the whole system is not going to work unless there is some what is technically called feedback where the court or legislative oversight committee keeps getting records regularly giving a comparison of the quantity and quality of the American messages being intercepted, the innocent American messages being intercepted, a comparison of that quantity and quality with the value of the legitimate take. There is going to have to be some sort of system that keeps bringing that back in.

**The CHAIRMAN.** It would seem to me that where you get into the legitimate foreign intelligence area that the introduction of a court device or the warrant device may indeed become very awkward. The best device would be an oversight committee of the Congress that would be kept fully informed and would pass judgment on these cases just to satisfy itself that these operations were being kept within proper guidelines and under proper restriction.

The trouble I have with the Attorney General's dissertation and his responses today is that he somehow seems to visualize that all of this could be done within the executive branch, that everything could be worked out with better procedures. Unless there is somebody checking on the executive branch that is not part of the executive branch and not subject to the ultimate control, direction and dismissal of the President, I do not think you have much protection.

**Mr. HEYMANN.** I certainly agree with that, Mr. Chairman. The only thing that I question in your statement is to whatever extent it involves a notion that entirely innocent, meaning nonforeign agent, American citizens can properly be monitored in their communications at home or from home to abroad simply because they are thought to possess in their minds intelligence which the CIA, or the NSA, or the State Department, or the Department of Defense, or the White House

would like to have. That is a notion which I believe on reflection the committee will find unpalatable. I must say I believe that, and a number of courts have acted whether it is in dictum quite acceptable. On reflection courts will not accept it. I think when the committee thinks hard about what it means—

The CHAIRMAN. In such cases you would require a warrant, or would you simply flatly prohibit?

Mr. HEYMANN. I would simply flatly prohibit a claim to own the mental—

The CHAIRMAN. That would be part of the definition. That would be part of the statutory exclusion from a definition of foreign intelligence.

Mr. HEYMANN. That is correct. In fact, the amendment that was written in 1789 or 1791 requires probable cause. Of course it has been extended and applies otherwise now.

The CHAIRMAN. Mr. Schwarz would like to ask a question.

Mr. SCHWARZ. Picking up on Senator Church's and your recognition of the hardest question, on a stream of communications, I understood your first point to be that if upon analysis the foreign intelligence value of the stream is not very great, even though it might exist, you say the stream could not be surveilled at all.

Mr. HEYMANN. If surveilling the stream requires a substantial invasion of the privacy of protected American communications.

Mr. SCHWARZ. Now let us assume that the stream does include significant, legitimate foreign intelligence—government to government—and in the course of analyzing, of obtaining that, it is technologically inevitable that one also obtains American citizens' messages. I want to put two different cases to you. One of those messages from an American citizen to an American citizen upon analysis contains evidence of a crime, although no one had any reason to suspect that before the stream was interrupted. The other message contains evidence of either economic matters or political matters. What do you do with those two messages that NSA or some other agency has now? Under your first principle, it was legitimate for the NSA to surveil the stream, and in the course of doing so it has acquired these two messages. What should they do with them?

Mr. KIRBOW. This is without a warrant?

Mr. SCHWARZ. There has been no warrant.

Mr. HEYMANN. My answer, Mr. Schwarz, is the traditional one. I believe it is the opposite of what the Attorney General suggested today. I think if the NSA legitimately reads a message which revealed itself as being evidence of a crime, keeps that message and seizes it, it has come upon it legitimately and is evidence of a crime. It keeps it and uses it and sends it to the FBI and it sends the people to jail. The other message that it reads that involves economic information, it has no right to. That is what I was urging upon Senator Church. That you have no right to take from American citizens what they happen to know just because the Government is interested in it, too.

One of my major differences with the Attorney General this morning was the notion that the fourth amendment particularly protects criminals, that its most important function is to exclude evidence against criminals. It was not written for that. It was written to protect

you and me. In your case I would send it directly to the FBI. I would send the message that indicated evidence of crime.

Mr. SCHWARZ. That you would send to the FBI, but the one economic or political—

Mr. HEYMANN. Would have to be destroyed immediately.

Mr. KIRBOW. Where do you attach the illegality? At the collection point, or the distribution point, or the machine where they supposedly sort all of this you are talking about?

Mr. HEYMANN. Let me take it in those three stages, Mr. Kirbow. I do not think that there is any search that is worth being called a search that would trouble anybody, either in looking at the envelopes for indicators, whatever they may be. I do not know what they are, or in going through voice or nonvoice traffic simply to cut down from 1 million items to 100,000 items which have the word assassination in them, let us say, or have the word North Korea in them. I do not think there is any search running those million items past somebody, only going so far. That does not seem to be a search.

The next step is the question as to whether you then have to read the 100,000 items along with the name of the sender and receiver. If it were technologically possible to do this somehow or another without getting the name of the sender and receiver, you could read the items. I think that there was just a limited search at the second stage. But if at the second stage, having cut yourself down to envelopes with indicators or some other kind of international traffic with selection criteria, if at that point you have to read the whole message or hear the whole message, together with the sender and receiver, there is very definitely a search at that point. You can minimize the effect of the search by thereafter discarding quickly whatever you have no right to.

Mr. KIRBOW. Do you mean to draw a distinction between reading the body of the message which I send as being different from one which I send if you read my signature as the sender and the addressee as the receiver? Do you draw a distinction between those two categories?

Mr. HEYMANN. I recognized it is idiosyncratic. I have not seen it anywhere else. When I think of it myself, I think I would feel quite differently. Let us take a letter, for example, about having a Government official read my letter, the body of my letter. If it were possible to eliminate who wrote it and who it is to, I would feel very differently about the privacy of that letter from a Government official reading it and knowing who it is from and who it is to.

Mr. KIRBOW. You are familiar with some of the technology of extremely high-speed transmissions, are you not? How do you distinguish there where they are almost instantaneously sent and then the signal goes off the air, and in that stream or volume of information when they are finally decoded on the other end, or smoothed out on the other end, we will call it by another mechanical device? How do you provide for such high-speed transmissions in this theory of yours as to what is legal? These are messages which make nothing but a sound as they go out over the air as you probably know. What do you do with those sort of things, which is the predominant way of sending secret information?

Mr. HEYMANN. I just have to go through the steps, Mr. Kirbow. There is no happy answer at the end of the steps. The first question is you have to identify conceptually what it is legitimate to pick up and

what it is not legitimate to pick up on that instantaneous stream, almost instantaneous stream. I have argued it is only legitimate to pick up foreign agents' traffic, foreign to foreign traffic, evidence-of-crime traffic, or something like that. First you have to identify what is illegitimate and what is legitimate. Then you ask yourself, is there any way that you can process this stream so to cut down the invasion of privacy to a minimum in the legitimate traffic that should not be intercepted?

You know, in the protected traffic, once you have done that and you explore every possibility for doing that, you do it by statute or by warrant. The next step is to say what is the balance between what is properly taken out of that and what is not? I agree with you. I think you are suggesting, Mr. Kirbow, when you are all through with that kind of fancy transmission, you're going to have a lot of useless stuff that you are allowed to take and a lot of stuff that you are not allowed to take when you are all through. At that point Congress and the courts are going to have to decide whether you are getting too much that is protected in order to get what you are legitimately allowed to take.

Mr. KIRBOW. Among the methods being used I do not see when the production comes you can review it as an aftereffect thing. I do not see how you are protecting the sender and receiver from an interception of the communication.

Mr. HEYMANN. I would require some kind of warrant in advance, unless Congress could handle that by statute, which I do not think the warrant procedure—I am shooting a little bit from the hip, Mr. Kirbow. I have only been thinking about it in the last few days since I started looking into it. The warrant procedure might say a court would itself pass on the selection criteria and the Congress might say use qualitative standards, saying the selection criteria should only be acceptable if they are so designed as to bring in highly important information of a foreign intelligence sort, proportionate in some way to the invasion of privacy. Then it could go on and Congress could add a second paragraph and say, even with these selection criteria, it can only be used if the following measures and minimization are used. Something like that.

Mr. KIRBOW. Thank you.

The CHAIRMAN. I think that we all recognize that this is a very complex matter when we are dealing with such advanced and rapidly changing technologies, and it leaves us all groping for new ways to keep old protections alive.

I think that your testimony has been very forthright and it has been very helpful. I want to thank you for it.

Mr. HEYMANN. Thank you very much.

The CHAIRMAN. That concludes the hearing today. We meet again in a public session at the call of the Chair.

[Whereupon, at 4:25 p.m., the hearing in the above-mentioned matter was concluded.]

HEARINGS EXHIBITS<sup>1</sup>

## EXHIBIT 1

FM YARBOROUGH ACS DA WASHINGTON

TO CARTER DIR OF NSA

1. AS YOU KNOW, THE DEPARTMENT OF THE ARMY IS, AND EXPECTS TO BE FOR SOMETIME TO COME, INVOLVED IN THE CIVIL DISTURBANCES TAKING PLACE WITHIN THE CONUS. WITH RESPECT TO THIS INVOLVEMENT, MY COUNTERINTELLIGENCE STAFF IS TASKED WITH KEEPING THE DA STAFF APPRISED OF THE COUNTERINTELLIGENCE MATTERS PERTAINING TO SUCH DISTURBANCES, INCLUDING INVOLVEMENT OF INDIVIDUALS AND ORGANIZATIONS. CONCERNING THE ANTI-VIETNAM DEMONSTRATION OF 21-22 OCTOBER 1967, THE DEPARTMENT OF THE ARMY HAS BEEN DESIGNATED AS THE EXECUTIVE AGENCY TO SUPPORT CIVILIAN AUTHORITIES WITH REGARD TO THIS ACTIVITY.
2. I AM PARTICULARLY INTERESTED IN DETERMINING WHETHER OR NOT THERE IS EVIDENCE OF ANY FOREIGN ACTION TO DEVELOP OR CONTROL THESE ANTI-VIETNAM AND OTHER DOMESTIC DEMONSTRATIONS. REALIZING, OF COURSE, THAT THIS IS THE "BIG" QUESTION, I NEVERTHELESS FEEL THAT WE SHOULD MAKE EVERY

<sup>1</sup> Under criteria determined by the Committee in consultation with the White House, the Departments of Defense and Justice, the National Security Agency, and the Federal Bureau of Investigation, certain materials have been deleted from these exhibits, which were previously classified, to maintain the integrity of the internal operating procedures of the agencies involved, and to protect sensitive communications intelligence sources and methods. Further deletions were made with respect to protecting the privacy of certain individuals and groups.

EFFORT TO OBTAIN THE ANSWER. SINCE YOUR AGENCY IS A MAJOR US INTELLIGENCE COLLECTOR, I WOULD APPRECIATE ANY INFORMATION ON A CONTINUING BASIS COVERING THE FOLLOWING:

A. INDICATIONS THAT FOREIGN GOVERNMENTS OR INDIVIDUALS AND ORGANIZATIONS ACTING AS AGENTS OF FOREIGN GOVERNMENTS ARE CONTROLLING OR ATTEMPTING TO CONTROL OR INFLUENCE THE ACTIVITIES OF US "PEACE" GROUPS AND "BLACK POWER" ORGANIZATIONS.

B. IDENTITIES OF FOREIGN AGENCIES EXERTING CONTROL OR INFLUENCE ON US ORGANIZATIONS.

C. IDENTITIES OF INDIVIDUALS AND ORGANIZATIONS IN US IN CONTACT WITH AGENTS OF FOREIGN GOVERNMENTS.

D. INSTRUCTIONS OR ADVICE BEING GIVEN TO US GROUPS BY AGENTS OF FOREIGN GOVERNMENTS.

3. FURTHER REQUEST THAT THIS OFFICE BE ADVISED WHEN ANY INDICATIONS ARE INTERCEPTED

BY NSA

DURING

THE NEXT THREE OR FOUR DAYS.

## EXHIBIT 2

FROM: DIRNSA

DATE: 28 OCTOBER 1967

TO: CIA, CHAIRMAN, USIB

CIA,

STATE/

/DIA,

ACSI DA, MAJ GEN WILLIAM P. YARBOROUGH

CNO.

AEC,

FBI,

IN RESPONSE TO A REQUEST FROM ACSI DA AND IAW DESIGNATION  
OF DA AS EXEC AGENT TO SUPPORT CIVIL AUTHORITIES WITH RESPECT  
TO CIVIL DISTURBANCES, WE ARE CONCENTRATING ADDITIONAL AND  
CONTINUING EFFORT TO OBTAIN SIGINT

TO NSA ON FOLLOWING:

A. INDICATIONS THAT FOREIGN GOVT'S OR INDIVIDUALS AND  
ORG'S ACTING AS AGENTS OF FOREIGN GOVT'S ARE CONTROLLING OR  
ATTEMPTING TO CONTROL OR INFLUENCE ACTIVITIES OF US "PEACE"  
GROUPS AND "BLACK POWER" ORGS.

B. IDENT'S OF FOREIGN AGENCIES EXERTING CONTROL OR  
INFLUENCE ON US ORGS.

C. IDENTITIES OF INDIVIDUALS AND ORGS IN US IN CONTACT  
WITH AGENTS OF FOR GOVT.

D. INSTRUCTIONS OR ADVICE BEING GIVEN TO US GROUPS  
BY AGENTS OF FOREIGN GOVT.

**2. YOU WILL BE ADVISED** **IN THE EVENT ANY SUCH**  
**INFO DEVELOPS FM SIGINT SOURCES.**

3.

EXHIBIT 3

Establishment of Sensitive SIGINT Operation  
Project MINARET (C)

DATE: 01 Jul 69

Project MINARET is  
Approved as a Sensitive SIGINT Operation.

Assistant Director, NSA

## CHARTER FOR SENSITIVE SIGINT OPERATION MINARET (C)

1. MINARET (C) is established for the purpose of providing more restrictive control and security of sensitive information derived from communications as processed which contain (a) information on foreign governments, organizations or individuals who are attempting to influence, coordinate or control U.S. organizations or individuals who may foment civil disturbances or otherwise undermine the national security of the U.S. (b) information on U.S. organizations or individuals who are engaged in activities which may result in civil disturbances or otherwise subvert the national security of the U.S. An equally important aspect of MINARET will be to restrict the knowledge that such information is being collected and processed by the National Security Agency.

2. MINARET specifically includes communications concerning individuals or organizations involved in civil disturbances, anti-war movements/demonstrations and military deserters involved in anti-war movements.

3. MINARET information will not be serialized, but will be identified for reference purposes by an assigned date/time. Information will be classified TOP SECRET, stamped "Background Use Only" and addressed to named recipients. Further, although MINARET will be handled as SIGINT and distributed to SIGINT recipients, it will not be identified with the National Security Agency.

## EXHIBIT 4

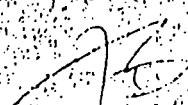
10 April 1970

MEMORANDUM FOR: The Director  
National Security Agency

SUBJECT: Request for NSA Assistance

This is to express my desire to receive information produced by your Agency which will assist the BNDD to more effectively combat the illicit traffic in narcotics and dangerous drugs. Attached you will find a requirement paper which I believe can serve as an initial statement of our need for pertinent reports published by NSA. Additional supplementary statements will be forwarded to you as appropriate to amplify our interest in more precise detail.

At this time, I wish to convey my most sincere appreciation for the hospitality and cooperation which was extended to my representative who recently conferred with Dr. Tordella and other NSA personnel on this subject.

  
JOHN B. INGERSOLL  
Director  
Bureau of Narcotics and  
Dangerous Drugs

Incl:  
a/s

MEMORANDUM FOR: Director, National Security Agency  
Ft. George G. Meade, Maryland

SUBJECT: Request for COMINT of Interest to  
Bureau of Narcotics and Dangerous  
Drugs (BNDD)

I. OBJECTIVE: To obtain Communications Intelligence information necessary to satisfactorily fulfill the mission of the BNDD.

II. BACKGROUND: The BNDD was established to more effectively combat the abuse of narcotics and dangerous drugs. The primary responsibility of the BNDD is to enforce the laws and statutes relating to narcotic drugs, marihuana, depressants, stimulants, and the hallucinogenic drugs. To achieve this goal the Bureau has stationed highly trained agents along the traditional routes of illicit traffic both in the United States and in foreign countries. Their objectives are to reach the highest possible sources of supply and to seize illicit drugs before they reach the abuser. The Bureau assists and cooperates with

State and local law enforcement agencies, legislators, and prosecutors, in the free exchange of information and mutual assistance aimed at the effective control of narcotics and dangerous drugs.

III. REQUIREMENTS:

1. The BNDD has a requirement for any and all COMINT information which reflects illicit traffic in narcotics and dangerous drugs. Our primary interest falls in the following categories:

- a) organizations engaged in such activities
- b) individuals engaged in such activities
- c) information on the distribution of narcotics and dangerous drugs
- d) information on cultivation and production centers
- e) international agreements and efforts to control the traffic in narcotics and dangerous drugs

f) all violations of the laws of the U. S. concerning narcotics and dangerous drugs

2. To assist NSA in the selection of pertinent COMINT information, the BNDD will provide a list of organizations and individuals with a history of illicit drug activities. This Watch List will be updated on a monthly basis and any additions/deletions will be forwarded to NSA. Any COMINT information developed on these individuals/organizations should be brought to the attention of the BNDD.

IV. USIB SIGINT PRIORITY:

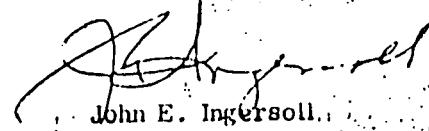
In consideration of the President's keen interest in eliminating the problem of drug abuse, it appears appropriate to include this requirement under Priority National Intelligence Objectives.

V. HANDLING PRECEDENCE:

Any information developed under this requirement should be released as appropriate in the judgment of the releasing authority.

VI. REVIEW DATE:

This requirement will be supplemented as warranted.  
A complete review will be made within one year of its acceptance.



John E. Ingersoll  
Director  
Bureau of Narcotics and Dangerous Drugs

## EXHIBIT 5



NATIONAL SECURITY AGENCY  
FORT GEORGE G. MEADE, MARYLAND 20755

26 January 1971

MEMORANDUM FOR THE SECRETARY OF DEFENSE  
THE ATTORNEY GENERAL

SUBJECT: NSA Contribution to Domestic Intelligence

Consistent with our conversation today, these are the agreed ground rules on NSA contribution to intelligence bearing on domestic problems.

Character

To be consistent with accepted standards in respect to protection of individual constitutional rights and civil liberties.

Source

Telecommunications with at least one foreign terminal.

Scope

Intelligence bearing on:

- (1) Criminal activity, including drugs.
- (2) Foreign support or foreign basing of subversive activity.
- (3) Presidential and related protection.

Procedures

Tasking by competent authority only.

Special procedures to protect source, to include:

- (1) Compartmented reporting to FBI or BNDD for criminal activity, to FBI and CIA for foreign-related subversive activity, and to the Secret Service for Presidential protection.

- (2) No indications of origin.
- (3) No evidential or other public use under any circumstances.
- (4) Screening at source (NSA) to insure compliance with the above criteria.

It is further understood that NSA will insure full availability of all relevant material by competent and informed representation in the Justice working group.

With warm regard,



NOEL GAYLER

Vice Admiral, U. S. Navy

Director

## EXHIBIT 6



NATIONAL SECURITY AGENCY  
FORT GEORGE G. MEADE, MARYLAND 20755

17 September 1973

The Honorable Clarence M. Kelley  
Director, Federal Bureau of Investigation  
Justice Building  
9th and Pennsylvania Avenue, NW  
Washington, D. C. 20535

Dear Mr. Kelley:

In the course of acclimating myself to my new assignment I asked my staff to review with yours our Watch List procedures, and they have been pursuing that subject diligently.

Meanwhile, I thought it would be worthwhile for us, as the heads of cooperating agencies, to correspond directly on the Watch List matter. The need for proper handling of the list and related information has intensified, along with ever-increasing pressures for disclosure of sources by the Congress, the courts, and the press, and naturally I am concerned ultimately for the protection of highly vulnerable SIGINT sources. Of paramount importance, however, is to insure that the procedures we have established for compiling the lists, and for changing them as needs dictate, remain adequate and fully appropriate to our authorities and responsibilities.

Certainly, I expect NSA to remain as responsive to your future requirements for information as we have to those of the past. Also, as in the past, we at NSA will lack the wherewithall for verifying the appropriateness of the Watch List entries, and we will continue to rely upon you, as the requesting agency, for that assurance. However, the requirement for us to perform the NSA mission in ways that remain unquestionably within the framework of our existing authorities has never been more clearly evident. I am confident that current procedures are designed to insure that we do so; however, I ask your help in my efforts to make doubly certain that in the process of our providing you Watch List information acquired during the performance of our foreign intelligence mission we do not — even inadvertently — exceed the letter or spirit of any controlling law or directive.

REC-2

It would be of great value to me in establifshing this kind of positive assurance if, at the earliest possible date, you will review the current list your agency has filed with us in order to satisfy yourself regarding the appropriateness of its contents, and if you will reaffirm for me the adequacy of your agency's procedures for making changes to it.

Sincerely,



LEW ALLEN, JR.  
Lieutenant General, USAF  
Director

## EXHIBIT 7

Office of the Attorney General  
Washington, D.C. 20530

October 1 1973

Lt. General Lew Allen, Jr., USAF  
Director  
National Security Agency  
Fort George G. Meade, Maryland 20755

Dear General Allen:

- It has recently come to my attention for the first time that your Agency is disseminating to the Federal Bureau of Investigation and the Secret Service information obtained by NSA by means of electronic surveillance.

Recently, the Supreme Court held, in a case entitled United States v. Keith, 407 U.S. 297, that the Federal Government could not conduct electronic surveillance on citizens of this country without a warrant in certain circumstances. The practice by NSA of conducting electronic surveillance at the request of an investigative agency and disseminating the information obtained thereby raises a number of serious legal questions which have yet to be resolved.

Until I am able more carefully to assess the effect of Keith and other Supreme Court decisions concerning electronic surveillance upon your current practice of

disseminating to the FBI and Secret Service information acquired by you through the use of electronic devices pursuant to requests from FBI and Secret Service, it is requested that you immediately curtail the further dissemination of such information to these agencies.

Of course, relevant information acquired by you in the routine pursuit of the collection of foreign intelligence information may continue to be furnished to appropriate Government agencies. What is to be avoided is NSA's responding to a request from another agency to monitor in connection with a matter that can only be considered one of domestic intelligence.

I will communicate with you further on this in the near future;

Sincerely,



Robert F. Kennedy  
Attorney General

## EXHIBIT 8



NATIONAL SECURITY AGENCY  
FORT GEORGE G. MEADE, MARYLAND 20755

4 October 1973

The Honorable Elliot L. Richardson  
Attorney General  
Washington, D. C. 20530

Dear Mr. Attorney General:

This replies to your letter of October 1, 1973 concerning the dissemination to the Federal Bureau of Investigation and the United States Secret Service of information derived from the interception of foreign communications.

Our missions include the production and dissemination of intelligence information in response to needs expressed to us by the United States Intelligence Board and its members. We carry out that mission in part by the interception of messages transmitted over certain foreign communications facilities.

[DELETED]

For some years, the FBI and the Secret Service have been asking us to provide, and we have been providing to them, copies of any messages contained in the foreign communications we intercept that bear on named individuals or organizations. These compilations of names are commonly referred to as "Watch Lists." No communications intercept activities have been conducted by NSA, and no cryptologic resources have been expended solely in order to acquire messages concerning names on the Watch Lists; those messages we acquire always are by-products of the foreign communications we intercept in the course of our legitimate and well recognized foreign intelligence activities.

The NSA has no facilities or charter that would allow it to ascertain whether specific Watch List entries are appropriate, and has always

depended upon the agencies compiling the lists to warrant that they are entitled, in the context of their authorities, to the information they request, and that the names they have entered on their Watch Lists are lawful objects of their inquiries, and are necessary and appropriate to their missions.

For this reason, I recently requested that Mr. Kelley and Mr. Rowley review and re-certify the lists they currently have on file here, and that they reaffirm the adequacy of their procedure for modifying the lists. They both have done this, and I plan to meet with each of them later in order to discuss in detail this same subject.

I believe that our current practice conforms to your guidance that, "relevant information acquired by you in the routine pursuit of the collection of foreign intelligence information may continue to be furnished to appropriate government agencies." However, to insure that our procedures are proper I request your consideration of providing the guidance you feel necessary to the FBI and the Secret Service for them to follow in the preparation of requests to NSA for information. I wish to add that the information we have provided appears to have been very useful to these agencies in the proper pursuit of their responsibilities.

In light of your concern, I have directed that no further information be disseminated to the FBI and Secret Service, pending advice on legal issues. I look forward to hearing further from you at an early date; in the meantime, I would be pleased to provide you whatever further detail might assist in your review.

Sincerely,



LEW ALLEN, JR.  
Lieutenant General, USAF  
Director

APPENDIX<sup>1</sup>

Office of the Attorney General  
Washington, D.C. 20530

NOV 11 1975

November 10, 1975

1975 NOV 12 PM 12:49  
SELECT COMMITTEE ON  
INTELLIGENCE ACTIVITIES

Honorable Richard S. Schweiker  
United States Senate  
Washington, D.C. 20510

Dear Senator Schweiker:

At the hearing before the Select Committee on Intelligence Activities, you asked me to comment on a specific provision from the FBI Manual of Rules and Regulations. As I told you at the hearing, through some misunderstanding, I had not seen that provision until almost immediately before the afternoon session of the Committee began and indeed while I was at the witness table. I did not have an opportunity to check the specific provision or to know about its origin. My statement that I was sure it did not represent present policy represented my firm belief.

I note that according to the press reports that a Bureau spokesman later in the day informed a reporter that the statement is still in the manual and that it does represent Bureau policy. I am writing this letter to you, with a copy to Senator Church, because I would not wish to mislead the Select Committee in any way.

I do believe, however, some further explanation is in order. First, the Bureau informs me that the provision has not been interpreted to mean that an investigation should not take place and that "any interpretation that an investigation would not be instituted because of the possibility of embarrassment to the Bureau was never intended and, in fact, has never been the policy of this Bureau." I am told that "what was intended to be conveyed was that in such eventuality FBI Headquarters desired to be advised of the matter before investigation is instituted so that Headquarters would be on notice and could direct the inquiry, if necessary."

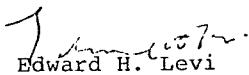
---

<sup>1</sup> See discussion on pp. 122-24.

Second, the manual provision dates back to March 30, 1955.

Third, I am informed by the Bureau that "immediate steps are being taken to remove that phraseology from our Manual of Rules and Regulations."

Sincerely,

  
Edward H. Levi

cc: Senator Church